2014-OCT-30
FSL version 7.5.643

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

17222 - (VMSA-2014-0010) VMware vCenter Server GNU Bash Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Description

Multiple vulnerabilities are present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

Multiple vulnerabilities are present in some versions of VMware vCenter Server. The flaws lie in the embedded version of Bash. Successful exploitation could allow an attacker to execute remote code.

17254 - Google Chrome Multiple Vulnerabilities Prior to 38.0.2125.101

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-3188, CVE-2014-3189, CVE-2014-3190, CVE-2014-3191, CVE-2014-3192, CVE-2014-3193, CVE-2014-3194, CVE-2014-3195, CVE-2014-3196, CVE-2014-3197, CVE-2014-3198, CVE-2014-3199, CVE-2014-3200

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose sensitive information or bypass security restrictions.

17255 - Google Chrome Multiple Vulnerabilities Prior to 38.0.2125.101

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3188, CVE-2014-3189, CVE-2014-3190, CVE-2014-3191, CVE-2014-3192, CVE-2014-3193, CVE-2014-3194, CVE-2014-3195, CVE-2014-3196, CVE-2014-3197, CVE-2014-3198, CVE-2014-3199, CVE-2014-3200

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose sensitive information or bypass security restrictions.

17264 - McAfee Web Gateway GNU Bash Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a popular enterprise Web solution.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaws lie in the embedded version of GNU Bash. Successful exploitation could allow an attacker to execute remote code.

17286 - Novell ZENworks Configuration Management GNU Bash Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Description

Multiple vulnerabilities are present in some versions of Novell ZENworks Configuration Management.

Observation

Novell ZENworks Configuration Management is a software product developed for computer systems management.

Multiple vulnerabilities are present in some versions of Novell ZENworks Configuration Management. The flaws lie in GNU Bash. Successful exploitation by a remote attacker could cause a denial of service and compromise a vulnerable system.

184594 - Ubuntu Linux 14.10 USN-2388-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6517, CVE-2014-6519, CVE-2014-6527, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
USN-2388-2

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-October/002706.html

Ubuntu 14.10

openjdk-7-jre-lib_7u71-2.5.3-0ubuntu1
openjdk-7-jre_7u71-2.5.3-0ubuntu1
openjdk-7-jre-zero_7u71-2.5.3-0ubuntu1
icedtea-7-jre-jamvm_7u71-2.5.3-0ubuntu1
openjdk-7-jre-headless_7u71-2.5.3-0ubuntu1

184596 - Ubuntu Linux 14.04 USN-2388-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6517, CVE-2014-6519, CVE-2014-6527, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
USN-2388-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-October/002705.html

Ubuntu 14.04

openjdk-7-jre-lib_7u71-2.5.3-0ubuntu0.14.04.1
openjdk-7-jre-headless_7u71-2.5.3-0ubuntu0.14.04.1
icedtea-7-jre-jamvm_7u71-2.5.3-0ubuntu0.14.04.1
openjdk-7-jre-zero_7u71-2.5.3-0ubuntu0.14.04.1
openjdk-7-jre_7u71-2.5.3-0ubuntu0.14.04.1

17214 - (SOL15629) F5 BIG-IP GNU Bash Code Injection Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Description

Multiple GNU Bash vulnerabilities are present in some versions of F5 BIG-IP systems.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

Multiple GNU Bash vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in the embedded version of GNU Bash. Successful exploitation could allow an attacker to execute remote code.

17265 - McAfee Network Data Loss Prevention GNU Bash Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Description

Multiple security vulnerabilities are present in some versions of McAfee Host Data Loss Prevention.

Observation

McAfee Host Data Loss Prevention monitors and prevents risky user behavior that can lead to a sensitive data breach.

Multiple security vulnerabilities are present in some versions of McAfee Host Data Loss Prevention. The flaws lie in the embedded version of Bash. Successful exploitation could allow an attacker to execute remote code or cause a denial of service condition.

17270 - Cisco ASA SQL*NET Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3382

Description

A vulnerability in some versions of Cisco ASA could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA could lead to a denial of service.

The flaw is due to improper handling of crafted SQL REDIRECT packets. Successful exploitation by a remote attacker could result in a denial of service condition.

17271 - Cisco ASA VPN Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3383

Description

A vulnerability in some versions of Cisco ASA could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA could lead to a denial of service.

The flaw is due to insufficient validation of UDP packets. Successful exploitation by a remote attacker could result in a denial of service condition.

17272 - Cisco ASA IKEv2 Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3384

Description

A vulnerability in some versions of Cisco ASA could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA could lead to a denial of service.

The flaw is due to improper handling of crafted IKEv2 packets. Successful exploitation by a remote attacker could result in a denial of service condition.

17273 - Cisco ASA Software VPN Failover Handler Privilege Escalation

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3389

Description

A vulnerability in some versions of Cisco Adaptive Security Appliance Software could lead to privilege escalation.

Observation

A vulnerability in some versions of Cisco Adaptive Security Appliance Software could lead to privilege escalation.

The flaw lies in the VPN code. Successful exploitation could allow a remote authenticated user gain elevated privileges.

17274 - Cisco ASA HPM ASDM Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3385

Description

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

The flaw lies in the Health and Performance Monitoring for ASDM feature. Successful exploitation by a remote attacker could result in a denial of service condition.

17275 - Cisco ASA GTP Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3386

Description

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

The flaw lies in the GPRS Tunneling Protocol inspection engine. Successful exploitation by a remote attacker could result in a denial of service condition.

17276 - Cisco ASA SunRPC Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3387

Description

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

The flaw lies in the SunRPC inspection engine. Successful exploitation by a remote attacker could result in a denial of service condition.

17301 - Cisco ASA DNS Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3388

Description

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco ASA Software could lead to a denial of service.

The flaw lies in the DNS inspection engine. Successful exploitation by a remote attacker could result in a denial of service condition.

17302 - Cisco ASA Software VNMC Command Input Validation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3390

Description

A vulnerability in some versions of Cisco ASA.

Observation

Cisco Adaptive Security Appliances (ASA) is a security and firewall device.

A vulnerability in some versions of Cisco ASA. The flaw lies in the Virtual Network Management Center (VNMC) policy implementation. Successful exploitation by a remote attacker could obtain Linux root access and executing a crafted script.

17304 - Cisco ASA Clientless SSL VPN Information Disclosure

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3392

Description

A vulnerability in some versions of Cisco ASA could lead to an information disclosure.

Observation

A vulnerability in some versions of Cisco ASA could lead to an information disclosure.

The flaw is due to insufficient sanitization of user-supplied input. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

91644 - Oracle Enterprise Linux ELSA-2014-1636 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-6457, CVE-2014-6468, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558, CVE-2014-6562

Description

The scan detected that the host is missing the following update:
ELSA-2014-1636

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2014-October/004573.html

OEL6
x86_64
java-1.8.0-openjdk-demo-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-javadoc-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-headless-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-devel-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-src-1.8.0.25-1.b17.el6

i386
java-1.8.0-openjdk-demo-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-javadoc-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-headless-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-devel-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-src-1.8.0.25-1.b17.el6

17321 - Oracle MySQL Multiple Vulnerabilities Prior To 5.5.40

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6464, CVE-2014-6469, CVE-2014-6491, CVE-2014-6494, CVE-2014-6496, CVE-2014-6500, CVE-2014-6507, CVE-2014-6555, CVE-2014-6559

Description

Multiple vulnerabilities are present in some versions of MySQL.

Observation

MySQL is an open source database server.

Multiple vulnerabilities are present in some versions of MySQL. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial of service or read/delete/modify sensitive data.

17325 - Oracle MySQL Multiple Vulnerabilities Prior To 5.6.21

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6464, CVE-2014-6469, CVE-2014-6491, CVE-2014-6494, CVE-2014-6496, CVE-2014-6500, CVE-2014-6507, CVE-2014-6555, CVE-2014-6559

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

MySQL is an open source database server.

Multiple vulnerabilities are present in some versions of MySQL. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial of service or read/delete/modify sensitive data.

93410 - Mandriva Linux MBS1 MDVSA-2014-210 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-6464, CVE-2014-6469, CVE-2014-6507, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
MDVSA-2014-210

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A210/

Mandriva Linux mbs1
x86_64
lib64mariadb-devel-5.5.40-1.1
lib64mariadb-embedded-devel-5.5.40-1.1
lib64mariadb-embedded18-5.5.40-1.1
lib64mariadb18-5.5.40-1.1
lib64jemalloc1-3.6.0-1
mariadb-core-5.5.40-1.1
lib64jemalloc-devel-3.6.0-1
mariadb-common-core-5.5.40-1.1
mariadb-client-5.5.40-1.1
mariadb-5.5.40-1.1
mariadb-bench-5.5.40-1.1
mariadb-obsolete-5.5.40-1.1
mariadb-extra-5.5.40-1.1
mysql-mariadb-5.5.40-1.1
mariadb-common-5.5.40-1.1
mariadb-feedback-5.5.40-1.1

142469 - SuSE SLES 11 SP3, SLED 11 SP3 xen-201409-9828 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-4344, CVE-2013-4540, CVE-2014-2599, CVE-2014-3967, CVE-2014-3968, CVE-2014-4021, CVE-2014-7154, CVE-2014-7155, CVE-2014-7156, CVE-2014-7188

Description

The scan detected that the host is missing the following update:
xen-201409-9828

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=yiSuV2SFDGE~
https://download.suse.com/Download?buildid=80Aj_aFfjUw~
https://download.suse.com/Download?buildid=DeWRKw_psgQ~
https://download.suse.com/Download?buildid=XtiNUQl9l6I~

SuSE SLED 11 SP3
x86_64
xen-libs-32bit-4.2.4_04-0.9.1
xen-4.2.4_04-0.9.1
xen-tools-domU-4.2.4_04-0.9.1
xen-doc-html-4.2.4_04-0.9.1
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.9.1
xen-tools-4.2.4_04-0.9.1
xen-libs-4.2.4_04-0.9.1
xen-doc-pdf-4.2.4_04-0.9.1

i586
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.9.1
xen-libs-4.2.4_04-0.9.1
xen-kmp-pae-4.2.4_04_3.0.101_0.40-0.9.1
xen-tools-domU-4.2.4_04-0.9.1

SuSE SLES 11 SP3
x86_64
xen-libs-32bit-4.2.4_04-0.9.1
xen-4.2.4_04-0.9.1
xen-tools-domU-4.2.4_04-0.9.1
xen-doc-html-4.2.4_04-0.9.1
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.9.1
xen-tools-4.2.4_04-0.9.1
xen-libs-4.2.4_04-0.9.1
xen-doc-pdf-4.2.4_04-0.9.1

i586
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.9.1
xen-libs-4.2.4_04-0.9.1
xen-kmp-pae-4.2.4_04_3.0.101_0.40-0.9.1
xen-tools-domU-4.2.4_04-0.9.1

17230 - (JSA10649) Juniper Junos OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3509, CVE-2014-3511, CVE-2014-3512, CVE-2014-5139

Description

Multiple vulnerabilities are present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper Junos. The flaws lie in OpenSSL component. Successful exploitation could allow an attacker to cause denial of service or unspecified other impact.

17303 - Cisco ASA Software Untrusted Search Path Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3391

Description

A vulnerability in some versions of Cisco ASA.

Observation

Cisco Adaptive Security Appliances (ASA) is a security and firewall device.

A vulnerability in some versions of Cisco ASA. The flaw lies in the function that exports environment variables. Successful exploitation allow an local users to gain privileges.

88642 - Slackware Linux 14.1 SSA:2014-296-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: High

CVE: CVE-2012-4412, CVE-2012-4424, CVE-2013-4237, CVE-2013-4458, CVE-2013-4788, CVE-2014-0475, CVE-2014-4043, CVE-2014-5119, CVE-2014-6040

Description

The scan detected that the host is missing the following update:
SSA:2014-296-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.647059

Slackware 14.1
x86_64
glibc-solibs-2.17-x86_64-8
glibc-profile-2.17-x86_64-8
glibc-i18n-2.17-x86_64-8
glibc-2.17-x86_64-8

noarch
glibc-zoneinfo-2014i-noarch-1

91645 - Oracle Enterprise Linux ELSA-2014-1654 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-3634

Description

The scan detected that the host is missing the following update:
ELSA-2014-1654

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2014-October/004562.html

OEL6
x86_64
rsyslog7-relp-7.4.10-3.el6_6
rsyslog7-7.4.10-3.el6_6
rsyslog7-elasticsearch-7.4.10-3.el6_6
rsyslog7-gssapi-7.4.10-3.el6_6
rsyslog7-mysql-7.4.10-3.el6_6
rsyslog7-pgsql-7.4.10-3.el6_6
rsyslog7-snmp-7.4.10-3.el6_6
rsyslog7-gnutls-7.4.10-3.el6_6

i386
rsyslog7-relp-7.4.10-3.el6_6
rsyslog7-7.4.10-3.el6_6
rsyslog7-elasticsearch-7.4.10-3.el6_6
rsyslog7-gssapi-7.4.10-3.el6_6
rsyslog7-mysql-7.4.10-3.el6_6
rsyslog7-pgsql-7.4.10-3.el6_6
rsyslog7-snmp-7.4.10-3.el6_6
rsyslog7-gnutls-7.4.10-3.el6_6

93407 - Mandriva Linux MBS1 MDVSA-2014-203 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-3566, CVE-2014-3567

Description

The scan detected that the host is missing the following update:
MDVSA-2014-203

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A203/

Mandriva Linux mbs1
x86_64
lib64openssl-static-devel-1.0.0o-1
openssl-1.0.0o-1
lib64openssl1.0.0-1.0.0o-1
lib64openssl-engines1.0.0-1.0.0o-1
lib64openssl-devel-1.0.0o-1

142467 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 kernel-9751 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1979, CVE-2014-1739, CVE-2014-2706, CVE-2014-3153, CVE-2014-4027, CVE-2014-4171, CVE-2014-4508, CVE-

2014-4667, CVE-2014-4943, CVE-2014-5077, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410

Description

The scan detected that the host is missing the following update:
kernel-9751

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=8_7d3PluUhs~
https://download.suse.com/Download?buildid=Z98S7020JK8~
https://download.suse.com/Download?buildid=VvbY-xM-FfE~

SuSE SLED 11 SP3
x86_64
kernel-xen-devel-3.0.101-0.40.1
kernel-xen-extra-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.7.3
kernel-default-extra-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-xen-base-3.0.101-0.40.1
kernel-xen-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

SuSE SLES 11 SP3
x86_64
kernel-xen-devel-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-ec2-base-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.7.3
kernel-xen-base-3.0.101-0.40.1
kernel-ec2-3.0.101-0.40.1
kernel-ec2-devel-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-xen-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

SuSE SLED 11
x86_64
kernel-xen-devel-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

SuSE SLES 11
x86_64
kernel-xen-devel-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

142471 - SuSE SLES 11 SP3 kernel-9748 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1979, CVE-2014-1739, CVE-2014-2706, CVE-2014-3153, CVE-2014-4027, CVE-2014-4171, CVE-2014-4508, CVE-2014-4667, CVE-2014-4943, CVE-2014-5077, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410

Description

The scan detected that the host is missing the following update:
kernel-9748

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=jEtHLjLpbf8~

SuSE SLES 11 SP3
ppc64
kernel-ppc64-base-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-ppc64-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-ppc64-devel-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

142472 - SuSE SLES 11 SP3 kernel-9749 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1979, CVE-2014-1739, CVE-2014-2706, CVE-2014-3153, CVE-2014-4027, CVE-2014-4171, CVE-2014-4508, CVE-2014-4667, CVE-2014-4943, CVE-2014-5077, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410

Description

The scan detected that the host is missing the following update:
kernel-9749

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

https://download.suse.com/Download?buildid=cZ_72vokYDs~

SuSE SLES 11 SP3
s390x
kernel-trace-base-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-default-man-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

142473 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 kernel-9746 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1979, CVE-2014-1739, CVE-2014-2706, CVE-2014-3153, CVE-2014-4027, CVE-2014-4171, CVE-2014-4508, CVE-2014-4667, CVE-2014-4943, CVE-2014-5077, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410

Description

The scan detected that the host is missing the following update:
kernel-9746

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=R494YaDQ2fg~
https://download.suse.com/Download?buildid=usaUxdVKYrU~
https://download.suse.com/Download?buildid=_8e2SZZX2f0~

SuSE SLED 11 SP3
i586
kernel-default-base-3.0.101-0.40.1
kernel-default-extra-3.0.101-0.40.1
kernel-pae-base-3.0.101-0.40.1
kernel-xen-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-xen-base-3.0.101-0.40.1
kernel-pae-extra-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-pae-devel-3.0.101-0.40.1
kernel-xen-extra-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
xen-kmp-pae-4.2.4_04_3.0.101_0.40-0.7.3
kernel-xen-3.0.101-0.40.1
kernel-pae-3.0.101-0.40.1
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.7.3

SuSE SLES 11 SP3
i586
kernel-default-base-3.0.101-0.40.1

kernel-pae-base-3.0.101-0.40.1
kernel-ec2-base-3.0.101-0.40.1
kernel-xen-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-xen-base-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-pae-devel-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-ec2-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
xen-kmp-pae-4.2.4_04_3.0.101_0.40-0.7.3
kernel-xen-3.0.101-0.40.1
kernel-ec2-devel-3.0.101-0.40.1
kernel-pae-3.0.101-0.40.1
xen-kmp-default-4.2.4_04_3.0.101_0.40-0.7.3

SuSE SLED 11
i586
kernel-xen-devel-3.0.101-0.40.1
kernel-pae-devel-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-pae-3.0.101-0.40.1
kernel-pae-base-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

SuSE SLES 11
i586
kernel-xen-devel-3.0.101-0.40.1
kernel-pae-devel-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-pae-3.0.101-0.40.1
kernel-pae-base-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-trace-base-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

142474 - SuSE SLES 11 SP3 kernel-9747 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1979, CVE-2014-1739, CVE-2014-2706, CVE-2014-3153, CVE-2014-4027, CVE-2014-4171, CVE-2014-4508, CVE-2014-4667, CVE-2014-4943, CVE-2014-5077, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410

Description

The scan detected that the host is missing the following update:
kernel-9747

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=crL5ZHbRv7w~

SuSE SLES 11 SP3
ia64
kernel-trace-base-3.0.101-0.40.1
kernel-trace-devel-3.0.101-0.40.1
kernel-source-3.0.101-0.40.1
kernel-trace-3.0.101-0.40.1
kernel-default-3.0.101-0.40.1
kernel-syms-3.0.101-0.40.1
kernel-default-base-3.0.101-0.40.1
kernel-default-devel-3.0.101-0.40.1

142475 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 kernel-bigsmp-201409-9750 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1979, CVE-2014-1739, CVE-2014-2706, CVE-2014-3153, CVE-2014-4027, CVE-2014-4171, CVE-2014-4508, CVE-2014-4667, CVE-2014-4943, CVE-2014-5077, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410

Description

The scan detected that the host is missing the following update:
kernel-bigsmp-201409-9750

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=fIuWsID3GpY~
https://download.suse.com/Download?buildid=YGsWT3c9UeE~
https://download.suse.com/Download?buildid=Nig38l4JlpM~

SuSE SLED 11 SP3
x86_64
kernel-bigsmp-devel-3.0.101-0.40.1

SuSE SLES 11 SP3
x86_64
kernel-bigsmp-devel-3.0.101-0.40.1
iscsitarget-kmp-bigsmp-1.4.20_3.0.101_0.40-0.38.83
oracleasm-kmp-bigsmp-2.0.5_3.0.101_0.40-7.39.89
kernel-bigsmp-3.0.101-0.40.1
ofed-kmp-bigsmp-1.5.4.1_3.0.101_0.40-0.13.89
kernel-bigsmp-base-3.0.101-0.40.1

SuSE SLED 11
x86_64
kernel-bigsmp-devel-3.0.101-0.40.1

SuSE SLES 11
x86_64
kernel-bigsmp-devel-3.0.101-0.40.1

170411 - Amazon Linux AMI ALAS-2014-433 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-4115, CVE-2014-0128, CVE-2014-3609

Description

The scan detected that the host is missing the following update:
ALAS-2014-433

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://alas.aws.amazon.com/ALAS-2014-433.html

Amazon Linux AMI
x86_64
squid-3.1.10-29.17.amzn1
squid-debuginfo-3.1.10-29.17.amzn1

i686
squid-3.1.10-29.17.amzn1
squid-debuginfo-3.1.10-29.17.amzn1

188401 - Fedora Linux 20 FEDORA-2014-13030 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-3704

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13030

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141512.html

Fedora Core 20

drupal7-7.32-1.fc20

188402 - Fedora Linux 19 FEDORA-2014-13031 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2011-4718, CVE-2013-4113, CVE-2013-4248, CVE-2013-6420, CVE-2014-0185, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:

FEDORA-2014-13031

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141404.html

Fedora Core 19

php-5.5.18-1.fc19

188406 - Fedora Linux 19 FEDORA-2014-13053 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-3704

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13053

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141436.html

Fedora Core 19

drupal7-7.32-1.fc19

188407 - Fedora Linux 20 FEDORA-2014-13013 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-6420, CVE-2014-0185, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13013

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141349.html

Fedora Core 20

php-5.5.18-1.fc20

17285 - (JSA10650) Juniper Junos SRX flowd ALG Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3825

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw is triggered when ALG is enabled and a especially crafted packet is processed by the flowd daemon. Successful exploitation may allow an attacker to cause a denial of service condition on the affected device.

17317 - Oracle MySQL Multiple Vulnerabilities Prior To 5.6.20

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-5615, CVE-2014-0224, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6474, CVE-2014-6478, CVE-2014-6484, CVE-2014-6489, CVE-2014-6495, CVE-2014-6505, CVE-2014-6530, CVE-2014-6551, CVE-2014-6564

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

MySQL is an open source database server.

Multiple vulnerabilities are present in some versions of MySQL. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial of service or read/delete/modify sensitive data.

58980 - Debian Linux 7.0 DSA-3055-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3694, CVE-2014-3695, CVE-2014-3696, CVE-2014-3698

Description

The scan detected that the host is missing the following update:
DSA-3055-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2014/dsa-3055

Debian 7.0
all
pidgin_2.10.10-1~deb7u1

58981 - Debian Linux 7.0 DSA-3056-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3467, CVE-2014-3468, CVE-2014-3469

Description

The scan detected that the host is missing the following update:
DSA-3056-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2014/dsa-3056

Debian 7.0
all
libtasn1-3_2.13-2+deb7u1

88641 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-296-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3694, CVE-2014-3695, CVE-2014-3696, CVE-2014-3697, CVE-2014-3698

Description

The scan detected that the host is missing the following update:
SSA:2014-296-02

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.540575

Slackware 13.0
x86_64
pidgin-2.10.10-x86_64-1

Slackware 14.1
x86_64
pidgin-2.10.10-x86_64-1

Slackware 13.37
x86_64
pidgin-2.10.10-x86_64-1

Slackware 13.1
x86_64
pidgin-2.10.10-x86_64-1

Slackware 14.0
x86_64
pidgin-2.10.10-x86_64-1

93406 - Mandriva Linux MBS1 MDVSA-2014-209 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
MDVSA-2014-209

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A209/

Mandriva Linux mbs1
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.65-2.5.3.1
java-1.7.0-openjdk-devel-1.7.0.65-2.5.3.1
java-1.7.0-openjdk-javadoc-1.7.0.65-2.5.3.1
java-1.7.0-openjdk-headless-1.7.0.65-2.5.3.1
java-1.7.0-openjdk-src-1.7.0.65-2.5.3.1
java-1.7.0-openjdk-demo-1.7.0.65-2.5.3.1
java-1.7.0-openjdk-1.7.0.65-2.5.3.1

93411 - Mandriva Linux MBS1 MDVSA-2014-202 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3670

Description

The scan detected that the host is missing the following update:
MDVSA-2014-202

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A202/

Mandriva Linux mbs1
x86_64
php-pdo_sqlite-5.5.18-1
php-doc-5.5.18-1
php-openssl-5.5.18-1
php-fpm-5.5.18-1
php-snmp-5.5.18-1
php-session-5.5.18-1
php-xmlwriter-5.5.18-1
php-phar-5.5.18-1
php-hash-5.5.18-1
php-xsl-5.5.18-1
php-mysql-5.5.18-1
php-ftp-5.5.18-1
php-cli-5.5.18-1
php-mbstring-5.5.18-1
php-ini-5.5.18-1

php-opcache-5.5.18-1
php-intl-5.5.18-1
php-iconv-5.5.18-1
php-cgi-5.5.18-1
php-xml-5.5.18-1
php-readline-5.5.18-1
php-json-5.5.18-1
php-xmlrpc-5.5.18-1
php-pcntl-5.5.18-1
apache-mod_php-5.5.18-1
php-bcmath-5.5.18-1
php-pdo_pgsql-5.5.18-1
php-pdo_dblib-5.5.18-1
php-pgsql-5.5.18-1
php-sysvshm-5.5.18-1
php-xmlreader-5.5.18-1
php-shmop-5.5.18-1
php-gd-5.5.18-1
php-pdo-5.5.18-1
php-curl-5.5.18-1
php-mysqli-5.5.18-1
php-odbc-5.5.18-1
php-pdo_mysql-5.5.18-1
php-calendar-5.5.18-1
php-soap-5.5.18-1
php-mysqlnd-5.5.18-1
php-pdo_odbc-5.5.18-1
php-zip-5.5.18-1
php-sysvmsg-5.5.18-1
php-ldap-5.5.18-1
php-fileinfo-5.5.18-1
php-tokenizer-5.5.18-1
php-devel-5.5.18-1
php-bz2-5.5.18-1
php-sqlite3-5.5.18-1
php-filter-5.5.18-1
php-apc-admin-3.1.15-1.12
php-gettext-5.5.18-1
php-mcrypt-5.5.18-1
php-exif-5.5.18-1
php-imap-5.5.18-1
php-ctype-5.5.18-1
php-apc-3.1.15-1.12
php-recode-5.5.18-1
php-gmp-5.5.18-1
php-dba-5.5.18-1
php-wddx-5.5.18-1
php-zlib-5.5.18-1
php-tidy-5.5.18-1
lib64php5_common5-5.5.18-1
php-sysvsem-5.5.18-1
php-posix-5.5.18-1
php-sybase_ct-5.5.18-1
php-dom-5.5.18-1
php-enchant-5.5.18-1
php-mssql-5.5.18-1
php-sockets-5.5.18-1

140594 - Red Hat Enterprise Linux RHSA-2014-1724 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-4653, CVE-2014-5077

Description

The scan detected that the host is missing the following update:
RHSA-2014-1724

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://rhn.redhat.com/errata/RHSA-2014-1724.html

RHEL7WS
x86_64
kernel-tools-libs-3.10.0-123.9.2.el7
kernel-headers-3.10.0-123.9.2.el7
kernel-debug-devel-3.10.0-123.9.2.el7
kernel-debug-debuginfo-3.10.0-123.9.2.el7
kernel-devel-3.10.0-123.9.2.el7
perf-3.10.0-123.9.2.el7
kernel-3.10.0-123.9.2.el7
python-perf-debuginfo-3.10.0-123.9.2.el7
perf-debuginfo-3.10.0-123.9.2.el7
kernel-tools-debuginfo-3.10.0-123.9.2.el7
kernel-debug-3.10.0-123.9.2.el7
kernel-debuginfo-common-x86_64-3.10.0-123.9.2.el7
kernel-tools-3.10.0-123.9.2.el7
kernel-debuginfo-3.10.0-123.9.2.el7

noarch
kernel-abi-whitelists-3.10.0-123.9.2.el7

RHEL7D
x86_64
kernel-tools-libs-3.10.0-123.9.2.el7
kernel-headers-3.10.0-123.9.2.el7
kernel-debug-devel-3.10.0-123.9.2.el7
kernel-debug-debuginfo-3.10.0-123.9.2.el7
kernel-devel-3.10.0-123.9.2.el7
perf-3.10.0-123.9.2.el7
kernel-3.10.0-123.9.2.el7
python-perf-debuginfo-3.10.0-123.9.2.el7
perf-debuginfo-3.10.0-123.9.2.el7
kernel-tools-debuginfo-3.10.0-123.9.2.el7
kernel-debug-3.10.0-123.9.2.el7
kernel-debuginfo-common-x86_64-3.10.0-123.9.2.el7
kernel-tools-3.10.0-123.9.2.el7
kernel-debuginfo-3.10.0-123.9.2.el7

noarch
kernel-abi-whitelists-3.10.0-123.9.2.el7

RHEL7S
x86_64
kernel-tools-libs-3.10.0-123.9.2.el7
kernel-headers-3.10.0-123.9.2.el7
kernel-debug-devel-3.10.0-123.9.2.el7

kernel-debug-debuginfo-3.10.0-123.9.2.el7
kernel-devel-3.10.0-123.9.2.el7
perf-3.10.0-123.9.2.el7
kernel-3.10.0-123.9.2.el7
python-perf-debuginfo-3.10.0-123.9.2.el7
perf-debuginfo-3.10.0-123.9.2.el7
kernel-tools-debuginfo-3.10.0-123.9.2.el7
kernel-debug-3.10.0-123.9.2.el7
kernel-debuginfo-common-x86_64-3.10.0-123.9.2.el7
kernel-tools-3.10.0-123.9.2.el7
kernel-debuginfo-3.10.0-123.9.2.el7

noarch
kernel-abi-whitelists-3.10.0-123.9.2.el7

142468 - SuSE Linux 12.3 openSUSE-SU-2014:1313-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3686

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1313-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2014-10/msg00027.html

SuSE Linux 12.3
i586
wpa_supplicant-1.1-2.4.1
wpa_supplicant-gui-debuginfo-1.1-2.4.1
wpa_supplicant-gui-1.1-2.4.1
wpa_supplicant-debugsource-1.1-2.4.1
wpa_supplicant-debuginfo-1.1-2.4.1

142470 - SuSE Linux 13.1 openSUSE-SU-2014:1314-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3686

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1314-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2014-10/msg00028.html

SuSE Linux 13.1

i586
wpa_supplicant-gui-debuginfo-2.0-3.8.1
wpa_supplicant-debuginfo-2.0-3.8.1
wpa_supplicant-2.0-3.8.1
wpa_supplicant-debugsource-2.0-3.8.1
wpa_supplicant-gui-2.0-3.8.1

174562 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1410-1973)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1410-1973)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=1973

SL7
x86_64
java-1.7.0-openjdk-headless-1.7.0.71-2.5.3.1.el7_0
java-1.7.0-openjdk-debuginfo-1.7.0.71-2.5.3.1.el7_0
java-1.7.0-openjdk-src-1.7.0.71-2.5.3.1.el7_0
java-1.7.0-openjdk-demo-1.7.0.71-2.5.3.1.el7_0
java-1.7.0-openjdk-devel-1.7.0.71-2.5.3.1.el7_0
java-1.7.0-openjdk-1.7.0.71-2.5.3.1.el7_0
java-1.7.0-openjdk-accessibility-1.7.0.71-2.5.3.1.el7_0

noarch
java-1.7.0-openjdk-javadoc-1.7.0.71-2.5.3.1.el7_0

SL6
x86_64
java-1.7.0-openjdk-demo-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-src-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-devel-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-debuginfo-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-1.7.0.71-2.5.3.1.el6

i386
java-1.7.0-openjdk-demo-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-src-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-devel-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-debuginfo-1.7.0.71-2.5.3.1.el6
java-1.7.0-openjdk-1.7.0.71-2.5.3.1.el6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.71-2.5.3.1.el6

174563 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1410-1306)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1410-1306)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=1306

SL5
x86_64
java-1.7.0-openjdk-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-src-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.71-2.5.3.1.el5_11

i386
java-1.7.0-openjdk-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-src-1.7.0.71-2.5.3.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.71-2.5.3.1.el5_11

174565 - Scientific Linux Security ERRATA Important: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1410-1820)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1410-1820)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=1820

SL7
x86_64
java-1.6.0-openjdk-src-1.6.0.33-1.13.5.0.el7_0
java-1.6.0-openjdk-demo-1.6.0.33-1.13.5.0.el7_0
java-1.6.0-openjdk-1.6.0.33-1.13.5.0.el7_0
java-1.6.0-openjdk-devel-1.6.0.33-1.13.5.0.el7_0
java-1.6.0-openjdk-debuginfo-1.6.0.33-1.13.5.0.el7_0
java-1.6.0-openjdk-javadoc-1.6.0.33-1.13.5.0.el7_0

SL6
x86_64
java-1.6.0-openjdk-demo-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-javadoc-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-devel-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-src-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-debuginfo-1.6.0.33-1.13.5.0.el6_6

i386
java-1.6.0-openjdk-demo-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-javadoc-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-devel-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-src-1.6.0.33-1.13.5.0.el6_6
java-1.6.0-openjdk-debuginfo-1.6.0.33-1.13.5.0.el6_6

SL5
x86_64
java-1.6.0-openjdk-src-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.33-1.13.5.0.el5_11

i386
java-1.6.0-openjdk-src-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.33-1.13.5.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.33-1.13.5.0.el5_11

181279 - FreeBSD libpurple/pidgin Multiple Vulnerabilities (d057c5e6-5b20-11e4-bebd-000c2980a9f3)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3694, CVE-2014-3695, CVE-2014-3696, CVE-2014-3697, CVE-2014-3698

Description

The scan detected that the host is missing the following update:
libpurple/pidgin -- multiple vulnerabilities (d057c5e6-5b20-11e4-bebd-000c2980a9f3)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/d057c5e6-5b20-11e4-bebd-000c2980a9f3.html

Affected packages:
libpurple < 2.10.10
pidgin < 2.10.10

184597 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2390-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3694, CVE-2014-3695, CVE-2014-3696, CVE-2014-3698

Description

The scan detected that the host is missing the following update:
USN-2390-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-October/002708.html

Ubuntu 14.10

pidgin_2.10.9-0ubuntu7.1
libpurple0_2.10.9-0ubuntu7.1

Ubuntu 14.04

libpurple0_2.10.9-0ubuntu3.2
pidgin_2.10.9-0ubuntu3.2

Ubuntu 12.04

pidgin_2.10.3-0ubuntu1.6
libpurple0_2.10.3-0ubuntu1.6

188413 - Fedora Linux 19 FEDORA-2014-11522 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-7185

Description

The scan detected that the host is missing the following update:
FEDORA-2014-11522

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141429.html

Fedora Core 19

python-2.7.5-14.fc19

17217 - Cisco ASA Software Version Information Disclosure

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3398

Description

A vulnerability in some versions of Cisco ASA could lead to an information disclosure.

Observation

A vulnerability in some versions of Cisco ASA could lead to an information disclosure.

The flaw is due to verbose output returned when a specific URL is submitted to the affected system. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

17282 - Joomla! Remote File Inclusion Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2014-7228

Description

A vulnerability is present in some versions of Joomla!.

Observation

Joomla! is a content management system.

A vulnerability is present in some versions of Joomla!. The flaws lie in multiple php files. Successful exploitation could allow the potential for remote files to be executed.

17283 - Joomla! Core Denial of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2014-7229

Description

A vulnerability is present in some versions of Joomla!.

Observation

Joomla! is a content management system.

A vulnerability is present in some versions of Joomla!. The flaws lie in multiple php files. Successful exploitation by a remote attacker could result in a denial of service condition.

17287 - (HT6531) Apple OS X Security Update 2014-005

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3566

Description

An information disclosure vulnerability is present in some versions of Apple OS X.

Observation

Apple OS X is an operating system used in Apple computer.

An information disclosure vulnerability is present in some versions of Apple OS X. The flaw lies in SSLv3 protocol. Successful exploitation could allow an attacker to obtain sensitive information.

17305 - Cisco ASA Clientless SSL VPN Portal Customization Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3393

Description

A vulnerability in some versions of Cisco ASA could lead to a security bypass.

Observation

A vulnerability in some versions of Cisco ASA could lead to a security bypass.

The flaw is due to improper implementation of authentication checks in the Clientless SSL VPN portal customization framework. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

17306 - Cisco ASA Smart Call Home Digital Certificate Validation Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3394

Description

A vulnerability in some versions of Cisco ASA could lead to a security bypass.

Observation

A vulnerability in some versions of Cisco ASA could lead to a security bypass.

The flaw exists because when SCH is configured, a trustpoint, including a VeriSign certificate, is automatically installed. Successful exploitation could allow a remote attacker to bypass intended access restrictions

17316 - (HPSBMU03118) HP Systems Insight Manager Multiple Vulnerabilities

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2643, CVE-2014-2644, CVE-2014-2645

Description

Multiple vulnerabilities are present in some versions of HP Systems Insight Manager.

Observation

HP Systems Insight Manager is a hardware management solution.

Multiple vulnerabilities are present in some versions of HP Systems Insight Manager. The flaws are caused due to unspecified errors. Successful exploitation could allow an attacker to bypass certain security restrictions, conduct clickjacking and cross-site scripting attacks.

17320 - (APSB14-23) Vulnerabilities In Adobe ColdFusion

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0570, CVE-2014-0571, CVE-2014-0572

Description

Multiple vulnerabilities are present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

Multiple vulnerabilities are present in some versions of Adobe ColdFusion. The flaws are caused due to unspecified errors. Successful exploitation could allow an attacker to bypass certain security restrictions, conduct cross-site scripting and cross-site request forgery attacks.

17322 - Oracle MySQL Multiple Vulnerabilities Prior To 5.5.39

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-5615, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6478, CVE-2014-6484, CVE-2014-6495, CVE-2014-6505, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551

Description

Multiple vulnerabilities are present in some versions of MySQL.

Observation

MySQL is an open source database server.

Multiple vulnerabilities are present in some versions of MySQL. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial of service or read/delete/modify sensitive data.

91646 - Oracle Enterprise Linux ELSA-2014-1677 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-6421, CVE-2014-6422, CVE-2014-6423, CVE-2014-6425, CVE-2014-6428, CVE-2014-6429, CVE-2014-6430, CVE-2014-6431, CVE-2014-6432

Description

The scan detected that the host is missing the following update:
ELSA-2014-1677

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2014-October/004571.html

OEL5
x86_64
wireshark-1.0.15-7.0.1.el5_11
wireshark-gnome-1.0.15-7.0.1.el5_11

i386
wireshark-1.0.15-7.0.1.el5_11
wireshark-gnome-1.0.15-7.0.1.el5_11

93408 - Mandriva Linux MBS1 MDVSA-2014-205 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-5461

Description

The scan detected that the host is missing the following update:
MDVSA-2014-205

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A205/

Mandriva Linux mbs1
x86_64
lib64lua5.1-5.1.4-11.1
lib64lua-static-devel-5.1.4-11.1
lib64lua5.0-devel-static-5.0.3-11.1
lib64lua5.0-5.0.3-11.1
lua5.0-5.0.3-11.1
lib64lua5.0-devel-5.0.3-11.1
lib64lua-devel-5.1.4-11.1
lua-5.1.4-11.1

93412 - Mandriva Linux MBS1 MDVSA-2014-207 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8760

Description

The scan detected that the host is missing the following update:
MDVSA-2014-207

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A207/

Mandriva Linux mbs1
x86_64
ejabberd-2.1.13-1.1
ejabberd-doc-2.1.13-1.1
ejabberd-devel-2.1.13-1.1

174564 - Scientific Linux Security ERRATA Moderate: openssh on SL6.x i386/x86_64 (1410-1694)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-2532, CVE-2014-2653

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssh on SL6.x i386/x86_64 (1410-1694)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=1694

SL6
x86_64
openssh-askpass-5.3p1-104.el6
openssh-server-5.3p1-104.el6
openssh-5.3p1-104.el6
openssh-clients-5.3p1-104.el6
pam_ssh_agent_auth-0.9.3-104.el6
openssh-debuginfo-5.3p1-104.el6
openssh-ldap-5.3p1-104.el6

i386
openssh-askpass-5.3p1-104.el6
openssh-server-5.3p1-104.el6
openssh-5.3p1-104.el6
openssh-clients-5.3p1-104.el6
pam_ssh_agent_auth-0.9.3-104.el6
openssh-debuginfo-5.3p1-104.el6
openssh-ldap-5.3p1-104.el6

174566 - Scientific Linux Security ERRATA Moderate: wireshark on SL6.x, SL7.x i386/x86_64 (1410-2400)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-6421, CVE-2014-6422, CVE-2014-6423, CVE-2014-6424, CVE-2014-6425, CVE-2014-6426, CVE-2014-6427, CVE-2014-6428, CVE-2014-6429, CVE-2014-6430, CVE-2014-6431, CVE-2014-6432

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: wireshark on SL6.x, SL7.x i386/x86_64 (1410-2400)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=2400

SL7
x86_64
wireshark-devel-1.10.3-12.el7_0
wireshark-gnome-1.10.3-12.el7_0
wireshark-debuginfo-1.10.3-12.el7_0
wireshark-1.10.3-12.el7_0

SL6
x86_64
wireshark-gnome-1.8.10-8.el6_6
wireshark-1.8.10-8.el6_6

wireshark-devel-1.8.10-8.el6_6
wireshark-debuginfo-1.8.10-8.el6_6

i386
wireshark-gnome-1.8.10-8.el6_6
wireshark-1.8.10-8.el6_6
wireshark-devel-1.8.10-8.el6_6
wireshark-debuginfo-1.8.10-8.el6_6

174567 - Scientific Linux Security ERRATA Moderate: wireshark on SL5.x i386/x86_64 (1410-1444)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-6421, CVE-2014-6422, CVE-2014-6423, CVE-2014-6425, CVE-2014-6428, CVE-2014-6429, CVE-2014-6430, CVE-2014-6431, CVE-2014-6432

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: wireshark on SL5.x i386/x86_64 (1410-1444)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=1444

SL5
x86_64
wireshark-1.0.15-7.el5_11
wireshark-gnome-1.0.15-7.el5_11
wireshark-debuginfo-1.0.15-7.el5_11

i386
wireshark-1.0.15-7.el5_11
wireshark-gnome-1.0.15-7.el5_11
wireshark-debuginfo-1.0.15-7.el5_11

174568 - Scientific Linux Security ERRATA Moderate: libxml2 on SL6.x, SL7.x i386/x86_64 (1410-2119)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libxml2 on SL6.x, SL7.x i386/x86_64 (1410-2119)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=2119

SL7
x86_64
libxml2-python-2.9.1-5.el7_0.1

libxml2-devel-2.9.1-5.el7_0.1
libxml2-2.9.1-5.el7_0.1
libxml2-static-2.9.1-5.el7_0.1
libxml2-debuginfo-2.9.1-5.el7_0.1

SL6
x86_64
libxml2-devel-2.7.6-17.el6_6.1
libxml2-2.7.6-17.el6_6.1
libxml2-python-2.7.6-17.el6_6.1
libxml2-static-2.7.6-17.el6_6.1
libxml2-debuginfo-2.7.6-17.el6_6.1

i386
libxml2-devel-2.7.6-17.el6_6.1
libxml2-2.7.6-17.el6_6.1
libxml2-python-2.7.6-17.el6_6.1
libxml2-static-2.7.6-17.el6_6.1
libxml2-debuginfo-2.7.6-17.el6_6.1

174569 - Scientific Linux Security ERRATA Low: trousers on SL6.x i386/x86_64 (1410-1572)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2012-0698

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: trousers on SL6.x i386/x86_64 (1410-1572)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=1572

SL6
x86_64
trousers-debuginfo-0.3.13-2.el6
trousers-0.3.13-2.el6
trousers-devel-0.3.13-2.el6
trousers-static-0.3.13-2.el6

i386
trousers-debuginfo-0.3.13-2.el6
trousers-0.3.13-2.el6
trousers-devel-0.3.13-2.el6
trousers-static-0.3.13-2.el6

174570 - Scientific Linux Security ERRATA Moderate: rsyslog5 and rsyslog on SL5.x, SL6.x i386/x86_64 (1410-2253)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2014-3634

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: rsyslog5 and rsyslog on SL5.x, SL6.x i386/x86_64 (1410-2253)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1410&L=scientific-linux-errata&T=0&P=2253

SL6
x86_64
rsyslog-5.8.10-9.el6_6
rsyslog-pgsql-5.8.10-9.el6_6
rsyslog-debuginfo-5.8.10-9.el6_6
rsyslog-snmp-5.8.10-9.el6_6
rsyslog-relp-5.8.10-9.el6_6
rsyslog-gnutls-5.8.10-9.el6_6
rsyslog-gssapi-5.8.10-9.el6_6
rsyslog-mysql-5.8.10-9.el6_6

i386
rsyslog-5.8.10-9.el6_6
rsyslog-pgsql-5.8.10-9.el6_6
rsyslog-debuginfo-5.8.10-9.el6_6
rsyslog-snmp-5.8.10-9.el6_6
rsyslog-relp-5.8.10-9.el6_6
rsyslog-gnutls-5.8.10-9.el6_6
rsyslog-gssapi-5.8.10-9.el6_6
rsyslog-mysql-5.8.10-9.el6_6

SL5
x86_64
rsyslog5-debuginfo-5.8.12-5.el5_11
rsyslog5-mysql-5.8.12-5.el5_11
rsyslog5-snmp-5.8.12-5.el5_11
rsyslog5-gssapi-5.8.12-5.el5_11
rsyslog5-pgsql-5.8.12-5.el5_11
rsyslog5-5.8.12-5.el5_11
rsyslog5-gnutls-5.8.12-5.el5_11

i386
rsyslog5-debuginfo-5.8.12-5.el5_11
rsyslog5-mysql-5.8.12-5.el5_11
rsyslog5-snmp-5.8.12-5.el5_11
rsyslog5-gssapi-5.8.12-5.el5_11
rsyslog5-pgsql-5.8.12-5.el5_11
rsyslog5-5.8.12-5.el5_11
rsyslog5-gnutls-5.8.12-5.el5_11

188409 - Fedora Linux 20 FEDORA-2014-13063 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-1833

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13063

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141446.html

Fedora Core 20

devscripts-2.14.10-1.fc20

188412 - Fedora Linux 20 FEDORA-2014-13302 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8088, CVE-2014-8089

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13302

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141480.html

Fedora Core 20

php-ZendFramework2-2.3.3-2.fc20

188416 - Fedora Linux 19 FEDORA-2014-12584 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-1571, CVE-2014-1572, CVE-2014-1573

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12584

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141309.html

Fedora Core 19

bugzilla-4.2.11-1.fc19

188419 - Fedora Linux 20 FEDORA-2014-12475 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-4346, CVE-2013-4347

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12475

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141492.html

Fedora Core 20

python-oauth2-1.5.211-8.fc20

188420 - Fedora Linux 19 FEDORA-2014-12536 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-4346, CVE-2013-4347

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12536

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141476.html

Fedora Core 19

python-oauth2-1.5.211-8.fc19

188421 - Fedora Linux 20 FEDORA-2014-12530 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-1571, CVE-2014-1572, CVE-2014-1573

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12530

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141321.html

Fedora Core 20

bugzilla-4.2.11-1.fc20

17308 - (HT6529) Apple OS X Server SSLv3 CBC Cipher Padding Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3566

Description

An information disclosure vulnerability is present in some versions of Apple OS X Server.

Observation

Apple Mac OS X Server provides easy to use interface to configure enterprise services for Apple devices.

An information disclosure vulnerability is present in some versions of Apple OS X Server. The flaw lies in the embedded version SSL 3.0. Successful exploitation may allow an attacker to access potentially sensitive information.

17309 - (HT6527) Apple OS X Server SSLv3 CBC Cipher Padding Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3566

Description

An information disclosure vulnerability is present in some versions of Apple OS X Server.

Observation

Apple Mac OS X Server provides easy to use interface to configure enterprise services for Apple devices.

An information disclosure vulnerability is present in some versions of Apple OS X Server. The flaw lies in the embedded version SSL 3.0. Successful exploitation may allow an attacker to access potentially sensitive information.

188408 - Fedora Linux 20 FEDORA-2014-13558 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-8086

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13558

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141471.html

Fedora Core 20

kernel-3.16.6-202.fc20

33277 - Oracle Solaris 150512-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
150512-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://getupdates.oracle.com/readme/150512-01

SunOS 5.8: bash patch

SOLARIS_8

SUNWbash:11.8.0,REV=2000.01.08.18.12

33278 - Oracle Solaris 150513-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
150513-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://getupdates.oracle.com/readme/150513-01

SunOS 5.8(x86): bash patch

SOLARIS_8_x86

SUNWbash:11.8.0,REV=2000.01.08.18.17

55235 - Top Weekly Malware Env - Trojan-Sysexp32 (Sysexp32.exe)

Category: Windows Host Assessment -> Top Weekly Malware
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is infected by the malware:
Env - Trojan-Sysexp32 (Sysexp32.exe)

Observation

This malware shows the following behavior:

The files and directories below were created:
%temp%\\Sysexp32.exe

For more information on this malware, visit http://vil.nai.com/vil/default.aspx

58979 - Debian Linux 7.0 DSA-3057-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
DSA-3057-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2014/dsa-3057

Debian 7.0
all
libxml2_2.8.0+dfsg1-7+wheezy2

58982 - Debian Linux 7.0 DSA-3058-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3684

Description

The scan detected that the host is missing the following update:
DSA-3058-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2014/dsa-3058

Debian 7.0
all
torque-client_2.4.16+dfsg-1+deb7u4
torque-mom_2.4.16+dfsg-1+deb7u4
libtorque2_2.4.16+dfsg-1+deb7u4
torque-client-x11_2.4.16+dfsg-1+deb7u4
torque-scheduler_2.4.16+dfsg-1+deb7u4
torque-server_2.4.16+dfsg-1+deb7u4
torque-common_2.4.16+dfsg-1+deb7u4
torque-pam_2.4.16+dfsg-1+deb7u4
libtorque2-dev_2.4.16+dfsg-1+deb7u4

93409 - Mandriva Linux MBS1 MDVSA-2014-204 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
MDVSA-2014-204

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A204/

Mandriva Linux mbs1
x86_64
lib64xml2-devel-2.7.8-14.20120229.2.5
lib64xml2_2-2.7.8-14.20120229.2.5
libxml2-utils-2.7.8-14.20120229.2.5
libxml2-python-2.7.8-14.20120229.2.5

181280 - FreeBSD phpMyAdmin XSS Vulnerabilities In SQL Debug Output And Server Monitor Page. (25b78f04-59c8-11e4-b711-6805ca0b3d42)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-8326

Description

The scan detected that the host is missing the following update:
phpMyAdmin -- XSS vulnerabilities in SQL debug output and server monitor page. (25b78f04-59c8-11e4-b711-6805ca0b3d42)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/25b78f04-59c8-11e4-b711-6805ca0b3d42.html

Affected packages:
4.2.0 <= phpMyAdmin < 4.2.10.1

184595 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2389-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
USN-2389-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-October/002707.html

Ubuntu 14.04

libxml2_2.9.1+dfsg1-3ubuntu4.4

Ubuntu 12.04

libxml2_2.7.8.dfsg-5.1ubuntu4.11

Ubuntu 10.04

libxml2_2.7.6.dfsg-1ubuntu1.15

184598 - Ubuntu Linux 14.04 USN-2387-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-2387-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-October/002704.html

Ubuntu 14.04

pollinate_4.7-0ubuntu1.2

188400 - Fedora Linux 20 FEDORA-2014-13773 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3610, CVE-2014-3611, CVE-2014-3646, CVE-2014-8369

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13773

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141478.html

Fedora Core 20

kernel-3.16.6-203.fc20

188403 - Fedora Linux 19 FEDORA-2014-12878 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3634

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12878

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141388.html

Fedora Core 19

sysklogd-1.5-18.fc19

188404 - Fedora Linux 20 FEDORA-2014-13040 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13040

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141493.html

Fedora Core 20

rubygem-httpclient-2.4.0-2.fc20

188405 - Fedora Linux 19 FEDORA-2014-13049 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13049

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141335.html

Fedora Core 19

java-1.8.0-openjdk-1.8.0.25-0.b18.fc19

188410 - Fedora Linux 19 FEDORA-2014-13027 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13027

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141347.html

Fedora Core 19

java-1.7.0-openjdk-1.7.0.71-2.5.3.0.fc19

188411 - Fedora Linux 20 FEDORA-2014-13521 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-8326

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13521

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141400.html

Fedora Core 20

phpMyAdmin-4.2.10.1-1.fc20

188414 - Fedora Linux 20 FEDORA-2014-12719 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12719

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141315.html

Fedora Core 20

perl-Mojolicious-5.49-1.fc20

188415 - Fedora Linux 20 FEDORA-2014-12308 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-7271, CVE-2014-7272

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12308

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141494.html

Fedora Core 20

sddm-0.9.0-2.20141007git6a28c29b.fc20

188417 - Fedora Linux 19 FEDORA-2014-12707 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12707

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141328.html

Fedora Core 19

perl-Mojolicious-5.49-1.fc19

188418 - Fedora Linux 20 FEDORA-2014-12910 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3634

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12910

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141380.html

Fedora Core 20

sysklogd-1.5-18.fc20

188422 - Fedora Linux 19 FEDORA-2014-13070 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13070

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-October/141488.html

Fedora Core 19

rubygem-httpclient-2.4.0-2.fc19

142466 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 perl-9858 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-4330

Description

The scan detected that the host is missing the following update:
perl-9858

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://download.suse.com/Download?buildid=x08Bo1yIjt0~
https://download.suse.com/Download?buildid=dW_oYtC9TSU~

https://download.suse.com/Download?buildid=cIF-hzeN7ds~
https://download.suse.com/Download?buildid=g25zThCO3Po~
https://download.suse.com/Download?buildid=Sjfr8gllE2c~
https://download.suse.com/Download?buildid=aGNzsYuENnk~
https://download.suse.com/Download?buildid=S6M-cIqFrqE~
https://download.suse.com/Download?buildid=0tJ0XchtAxY~
https://download.suse.com/Download?buildid=Em2MBT-GyxA~

SuSE SLED 11 SP3
x86_64
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1
perl-32bit-5.10.0-64.70.1

i586
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1

SuSE SLES 11 SP3
x86_64
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1
perl-32bit-5.10.0-64.70.1

i586
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1

SuSE SLED 11
x86_64
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1
perl-32bit-5.10.0-64.70.1

i586
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1

SuSE SLES 11
x86_64
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1

perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1
perl-32bit-5.10.0-64.70.1

i586
perl-5.10.0-64.70.1
perl-Module-Build-0.2808.01-0.70.1
perl-Test-Simple-0.72-0.70.1
perl-base-5.10.0-64.70.1
perl-doc-5.10.0-64.70.1

17291 - Oracle VM VirtualBox Critical Patch Update October 2014

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2014-6540

Description

A denial of service vulnerability is present in some versions of Oracle VirtualBox.

Observation

Oracle VirtualBox is a virtualization software.

A denial of service vulnerability is present in some versions of Oracle VirtualBox. The flaw is due to an error in the Graphics driver for Windows guests. Successful exploitation by a local attacker could cause a denial of service.

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

2562 - (MS04-024) Microsoft Windows Shell Internet Explorer Spoofing

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0211, CVE-2004-0216, CVE-2004-0420, CVE-2004-0727

Update Details

Recommendation is updated

2565 - (MS04-032) Microsoft Windows Kernel Metafiles Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0207, CVE-2004-0208, CVE-2004-0209, CVE-2004-0211, CVE-2004-0839, CVE-2004-0844

Update Details

Recommendation is updated

2687 - (MS04-034) Microsoft Windows Shell ZIP Directory Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0575

Update Details

Recommendation is updated

2808 - (MS04-036) Microsoft Windows NNTP Remote Code Execution Non-Intrusive

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0574

Update Details

Recommendation is updated

2809 - (MS04-035) Microsoft Windows SMTP DNS Lookup Remote Code Execution Non-Intrusive

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0840

Update Details

Recommendation is updated

2980 - (MS05-003) Microsoft Windows Index Service Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0897

Update Details

Recommendation is updated

2982 - (MS04-043) Microsoft Windows Hyper Terminal Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0568

Update Details

Recommendation is updated

2984 - (MS04-045) Microsoft Windows WINS Server Remote Code Execution and Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0567, CVE-2004-1080

Update Details

Recommendation is updated

2985 - (MS04-041) Microsoft Windows Word Pad Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0571, CVE-2004-0901

Update Details

Recommendation is updated

3135 - (MS05-009) Microsoft Windows Messenger LibPNG Multiple Issues

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0597, CVE-2004-0598

Update Details

Recommendation is updated

3339 - (MS05-019) Microsoft Windows TCP-IP Stack Code Execution and Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0230, CVE-2004-0790, CVE-2004-1060, CVE-2005-0048, CVE-2005-0065, CVE-2005-0066, CVE-2005-0067, CVE-2005-0068, CVE-2005-0356, CVE-2005-0688

Update Details

Recommendation is updated

3341 - (MS05-018) Microsoft Windows Kernel Privilege Escalation and Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0060, CVE-2005-0061, CVE-2005-0550, CVE-2005-0551

Update Details

Recommendation is updated

3342 - (MS05-017) Microsoft Windows Message Queue Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0059

Update Details

Recommendation is updated

3344 - (MS05-023) Microsoft Word 2000 Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0963, CVE-2005-0558

Update Details

Recommendation is updated

3345 - (MS05-023) Microsoft Word 2002 Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0963, CVE-2005-0558

Update Details

Recommendation is updated

3346 - (MS05-023) Microsoft Word 2003 Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0963, CVE-2005-0558

Update Details

Recommendation is updated

3658 - (MS05-039) Microsoft Windows SMB PnP Manager Remote Code Execution Null Session

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2005-1983, CVE-2005-1984

Update Details

Recommendation is updated

3893 - (MS05-049) Microsoft Windows Ink Shell Handling

Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-2117, CVE-2005-2118, CVE-2005-2122

Update Details

Recommendation is updated

4361 - (MS06-015) Microsoft Windows Explorer Remote COM Activation desktop.ini Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-2289, CVE-2006-0012

Update Details

Recommendation is updated

4364 - (MS06-013) Microsoft Internet Explorer HTML Parsing Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4365 - (MS06-013) Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1186, CVE-2006-1185, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4369 - (MS06-013) Microsoft Internet Explorer Cross-Domain Information Disclosure Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1191, CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4370 - (MS06-013) Microsoft Internet Explorer Address Bar Spoofing Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1192, CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4372 - (MS06-015) Microsoft Windows Explorer Remote COM Activation by GUID Folder Name Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0012, CVE-2004-2289

Update Details

Recommendation is updated

4417 - (MS06-030) Microsoft Server Message Block Driver Privilege Escalation (914389)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2373, CVE-2006-2374

Update Details

Recommendation is updated

4418 - (MS06-030) Microsoft Server Message Block Invalid Handle Vulnerability (917159)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2373, CVE-2006-2374

Update Details

Recommendation is updated

4501 - (MS06-041) Microsoft DNS Client Buffer Overrun Vulnerability (KB920683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3441, CVE-2006-3440

Update Details

Recommendation is updated

4700 - (MS05-049) Microsoft Windows lnk Filename Shell Handling

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-2117, CVE-2005-2118, CVE-2005-2122

Update Details

Recommendation is updated

4701 - (MS05-049) Microsoft Windows Web View Script Injection

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-2117, CVE-2005-2118, CVE-2005-2122

Update Details

Recommendation is updated

4944 - (MS07-016) Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability I (928090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4697, CVE-2007-0217, CVE-2007-0219

Update Details

Recommendation is updated

4945 - (MS07-016) Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability II (928090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4697, CVE-2007-0217, CVE-2007-0219

Update Details

Recommendation is updated

4974 - (MS07-037) Microsoft Publisher Invalid Memory Reference Vulnerability (936548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1754, CVE-2007-1117

Update Details

Recommendation is updated

5058 - (MS07-018) Microsoft Cross-site Scripting and Spoofing Vulnerability in Microsoft CMS Vulnerability (925939)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0939, CVE-2007-0938

Update Details

Recommendation is updated

5127 - (MS07-026) Microsoft Outlook Web Access Script Injection Vulnerability (931832)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0036, CVE-2007-0039, CVE-2007-0213, CVE-2007-0220, CVE-2007-0221

Update Details

Recommendation is updated

5128 - (MS07-026) Microsoft Malformed iCal Vulnerability (931832)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0036, CVE-2007-0039, CVE-2007-0213, CVE-2007-0220, CVE-2007-0221

Update Details

Recommendation is updated

5130 - (MS07-026) Microsoft IMAP Literal Processing Vulnerability (931832)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0036, CVE-2007-0039, CVE-2007-0213, CVE-2007-0220, CVE-2007-0221

Update Details

Recommendation is updated

5328 - (MS07-039) Microsoft Windows Active Directory Remote Code Execution Vulnerability (926122)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0040, CVE-2007-3028

Update Details

Recommendation is updated

5622 - (MS07-063) Microsoft SMBv2 Signing Vulnerability (942624)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5351

Update Details

Recommendation is updated

5698 - (MS08-006) Microsoft ASP Vulnerability (942830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0075

Update Details

Recommendation is updated

5699 - (MS08-007) Microsoft Mini-Redirector Heap Overflow Vulnerability (946026)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0080

Update Details

Recommendation is updated

5700 - (MS08-008) Microsoft OLE Heap Overrun Vulnerability (947890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0065

Update Details

Recommendation is updated

5708 - (MS08-012) Microsoft Publisher Invalid Memory Reference Vulnerability (947085)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0102, CVE-2008-0104

Update Details

Recommendation is updated

5709 - (MS08-012) Microsoft Publisher Memory Corruption (947085)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0102, CVE-2008-0104

Update Details

Recommendation is updated

6063 - (MS08-050) Microsoft Messenger Information Disclosure Vulnerability (946648)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0082

Update Details

Recommendation is updated

6160 - (MS08-059) Microsoft HIS Code Execution Vulnerability (956695)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3466

Update Details

Recommendation is updated

6163 - (MS08-063) Microsoft SMB Buffer Underflow Vulnerability (957095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4038

Update Details

Recommendation is updated

6165 - (MS08-060) Microsoft Active Directory Overflow Vulnerability (957280)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4023

Update Details

Recommendation is updated

6292 - (MS08-076) Microsoft Windows Media Components ISATAP Vulnerability (959807)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3010

Update Details

Recommendation is updated

6293 - (MS08-076) Microsoft Windows Media Components SPN Vulnerability (959807)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3009

Update Details

Recommendation is updated

6374 - (MS09-001) SMB Buffer Overflow Remote Code Execution Vulnerability (958687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4834

Update Details

Recommendation is updated

6375 - (MS09-001) SMB Validation Remote Code Execution Vulnerability (958687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4835

Update Details

Recommendation is updated

6605 - (MS09-013) Microsoft Windows HTTP Services Integer Underflow Vulnerability (960803)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0086

Update Details

Recommendation is updated

6742 - (MS09-018) Microsoft Windows Active Directory Invalid Free Vulnerability (971055)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1138

Update Details

Recommendation is updated

6761 - (MS09-022) Microsoft Windows Buffer Overflow in Print Spooler Vulnerability (961501)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0228

Update Details

Recommendation is updated

6770 - (MS09-026) Microsoft Windows RPC Marshalling Engine Vulnerability (970238)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0568

Update Details

Recommendation is updated

6954 - (MS09-042) Microsoft Telnet Credential Reflection Vulnerability (960859)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1930

Update Details

Recommendation is updated

6958 - (MS09-037) Microsoft ATL Object Type Mismatch Vulnerability (973908)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2494

Update Details

Recommendation is updated

7188 - (MS09-050) SMBv2 Command Value Vulnerability (975517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2532

Update Details

Recommendation is updated

7219 - (MS09-050) Vulnerabilities In SMBv2 Could Allow Remote Code Execution (975517)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3103

Update Details

Recommendation is updated

7220 - (MS09-051) Vulnerabilities In Windows Media Runtime Could Allow Remote Code Execution (975682)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0555, CVE-2009-2525

Update Details

Recommendation is updated

7221 - (MS09-052) Vulnerability In Windows Media Player Could Allow Remote Code Execution (974112)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2527

Update Details

Recommendation is updated

7223 - (MS09-062) Vulnerabilities In GDI+ Could Allow Remote Code Execution (957488)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2500, CVE-2009-2501, CVE-2009-2502, CVE-2009-2503, CVE-2009-2504, CVE-2009-2518, CVE-2009-2528, CVE-2009-3126

Update Details

Recommendation is updated

7224 - (MS09-054) Cumulative Security Update For Internet Explorer (974455)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1547, CVE-2009-2529, CVE-2009-2530, CVE-2009-2531

Update Details

Recommendation is updated

7225 - (MS09-061) Vulnerabilities In The Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0090, CVE-2009-0091, CVE-2009-2497

Update Details

Recommendation is updated

7226 - (MS09-060) Vulnerabilities In Microsoft ATL ActiveX Controls For Microsoft Office Could Allow Remote Code Execution (973965)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0901, CVE-2009-2493, CVE-2009-2495

Update Details

Recommendation is updated

7314 - (MS09-064) Vulnerability in License Logging Server Could Allow Remote Code Execution (974783)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2523

Update Details

Recommendation is updated

7329 - (MS09-064) Vulnerability in License Logging Server Could Allow Remote Code Execution (974783)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2009-2523

Update Details

Recommendation is updated

7332 - (MS09-065) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1127, CVE-2009-2513, CVE-2009-2514

Update Details

Recommendation is updated

7350 - (MS09-002) Cumulative Security Update For Internet Explorer (961260)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0075, CVE-2009-0076

Update Details

Recommendation is updated

7421 - (MS09-037) Vulnerabilities In Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0015, CVE-2008-0020, CVE-2009-0901, CVE-2009-2493, CVE-2009-2494

Update Details

Recommendation is updated

7426 - (MS09-042) Vulnerability In Telnet Could Allow Remote Code Execution (960859)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1930

Update Details

Recommendation is updated

7452 - (MS09-071) Memory Corruption in Internet Authentication Service Vulnerability (974318)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2505

Update Details

Recommendation is updated

7453 - (MS09-071) MS-CHAP Authentication Bypass in Internet Authentication Service Vulnerability (974318)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3677

Update Details

Recommendation is updated

7463 - (MS09-071) Vulnerabilities In Internet Authentication Service Could Allow Remote Code Execution (974318)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2505, CVE-2009-3677

Update Details

Recommendation is updated

7545 - (MS09-026) Vulnerability In RPC Could Allow Elevation Of Privilege (970238)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0568

Update Details

Recommendation is updated

7637 - (MS08-050) Vulnerability In Windows Messenger Could Allow Information Disclosure (955702)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0082

Update Details

Recommendation is updated

7680 - (MS08-060) Vulnerability In Active Directory Could Allow Remote Code Execution (957280)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4023

Update Details

Recommendation is updated

7705 - (MS08-006) Vulnerability In Internet Information Services Could Allow Remote Code Execution (942830)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0075

Update Details

Recommendation is updated

7731 - (MS08-024) Cumulative Security Update For Internet Explorer (947864)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1085

Update Details

Recommendation is updated

7736 - (MS08-026) Vulnerabilities In Microsoft Word Could Allow Remote Code Execution (951207)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1091, CVE-2008-1434

Update Details

Recommendation is updated

7743 - (MS10-002) Cumulative Security Update For Internet Explorer (978207)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

7770 - (MS08-007) Vulnerability In WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0080

Update Details

Recommendation is updated

7771 - (MS08-008) Vulnerability In OLE Automation Could Allow Remote Code Execution (947890)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0065

Update Details

Recommendation is updated

7883 - (MS10-009) Vulnerabilities In Windows TCP/IP Could Allow Remote Code Execution (974145)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0239, CVE-2010-0240, CVE-2010-0241, CVE-2010-0242

Update Details

Recommendation is updated

7939 - (MS08-014) Vulnerabilities In Microsoft Excel Could Allow Remote Code Execution (949029)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

8041 - (MS08-059) Vulnerability In Host Integration Server RPC Service Could Allow Remote Code Execution (956695)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3466

Update Details

Recommendation is updated

8053 - (MS08-063) Vulnerability in SMB Could Allow Remote Code Execution (957095)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4038

Update Details

Recommendation is updated

8131 - (MS08-065) Vulnerability In Message Queuing Could Allow Remote Code Execution (951071)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3479

Update Details

Recommendation is updated

8392 - (MS08-076) Vulnerabilities In Windows Media Components Could Allow Remote Code Execution (959807)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3009, CVE-2008-3010

Update Details

Recommendation is updated

8529 - (MS10-020) Microsoft Windows SMB Client Memory Allocation Vulnerability (980232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0269

Update Details

Recommendation is updated

8530 - (MS10-020) Microsoft Windows SMB Client Transaction Vulnerability (980232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0270

Update Details

Recommendation is updated

8531 - (MS10-020) Microsoft Windows SMB Client Response Parsing Vulnerability (980232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0476

Update Details

Recommendation is updated

8532 - (MS10-020) Microsoft Windows SMB Client Message Size Vulnerability (980232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0477

Update Details

Recommendation is updated

9070 - (MS10-040) Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1256

Update Details

Recommendation is updated

9688 - (MS10-054) Microsoft Windows SMB Pool Overflow Remote Code Execution (982214)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2550

Update Details

Recommendation is updated

10939 - (MS11-004) Microsoft IIS FTP Service Heap Buffer Overrun (2489256)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3972

Update Details

Recommendation is updated

11823 - (MS11-020) Microsoft SMB Transaction Parsing Remote Code Execution (2508429)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0661

Update Details

Recommendation is updated

11825 - (MS11-019) Microsoft Browser Pool Corruption Remote Code Execution (2511455)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0654

Update Details

Recommendation is updated

11837 - (MS11-019) Microsoft Browser Pool Corruption Remote Code Execution (2511455)

Category: General Vulnerability Assessment -> Instrusive -> Windows

Risk Level: High

CVE: CVE-2011-0654

Update Details

Recommendation is updated

12206 - (MS11-043) Microsoft Windows SMB Client Could Allow Remote Code Execution (KB2536276)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1268

Update Details

Recommendation is updated

12218 - (MS11-040) Microsoft Windows Threat Management Gateway Firewall Client Could Allow Remote Code Execution (KB2520426)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1889

Update Details

Recommendation is updated

12220 - (MS11-042) Microsoft Windows DFS Memory Corruption Remote Code Execution (2535512)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1868

Update Details

Recommendation is updated

12229 - (MS11-043) Microsoft Windows SMB Client Could Allow Remote Code Execution (KB2536276)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1268

Update Details

Recommendation is updated

12323 - (MS11-053) Microsoft Windows Bluetooth Stack Error Allow Remote Code Execution (2566220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1265

Update Details

Recommendation is updated

12339 - (MS11-053) Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (2566220)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1265

Update Details

Recommendation is updated

12456 - (MS11-058) Microsoft DNS Server NAPTR Query Could Allow Remote Code Execution (2562485)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1966

Update Details

Recommendation is updated

12915 - (MS11-083) Microsoft Windows Reference Counter Overflow Remote Code Execution (2588516)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2013

Update Details

Recommendation is updated

12916 - (MS11-083) Vulnerability in Microsoft Windows Reference Counter Overflow Remote Code Execution (2588516)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2013

Update Details

Recommendation is updated

14021 - (MS12-054) Microsoft Windows Networking Components Remote Administration Protocol Remote Code Execution II (2733594)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1853

Update Details

Recommendation is updated

14022 - (MS12-054) Microsoft Windows Networking Components Remote Administration Protocol Remote Code Execution (2733594)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1852

Update Details

Recommendation is updated

14023 - (MS12-054) Microsoft Windows Networking Components Print Spooler Service Remote Code Execution (2733594)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1851

Update Details

Recommendation is updated

14377 - (MS12-075) Microsoft Windows Font Parsing Remote Code Execution (2761226)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2897

Update Details

Recommendation is updated

14381 - (MS12-075) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2530, CVE-2012-2553, CVE-2012-2897

Update Details

Recommendation is updated

14495 - (MS12-078) Microsoft Windows True Type Font Parsing Remote Code Execution (2783534)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4786

Update Details

Recommendation is updated

14501 - (MS12-078) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2556, CVE-2012-4786

Update Details

Recommendation is updated

14715 - (MS13-015) Microsoft .NET Framework WinForms Callback Privilege Escalation (2800277)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0073

Update Details

Recommendation is updated

16018 - (MS13-105) Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2915705)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1330, CVE-2013-5072, CVE-2013-5763, CVE-2013-5791

Update Details

Recommendation is updated

16710 - (MS14-035) Cumulative Security Update for Internet Explorer (2969262)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0282, CVE-2014-1762, CVE-2014-1764, CVE-2014-1766, CVE-2014-1769, CVE-2014-1770, CVE-2014-1771, CVE-2014-1772, CVE-2014-1773, CVE-2014-1774, CVE-2014-1775, CVE-2014-1777, CVE-2014-1778, CVE-2014-1779, CVE-2014-1780, CVE-2014-1781, CVE-2014-1782, CVE-2014-1783, CVE-2014-1784, CVE-2014-1785, CVE-2014-1786, CVE-2014-1788, CVE-2014-1789, CVE-2014-1790, CVE-2014-1791, CVE-2014-1792, CVE-2014-1794, CVE-2014-1795, CVE-2014-1796, CVE-2014-1797, CVE-2014-1799, CVE-2014-1800, CVE-2014-1802, CVE-2014-1803, CVE-2014-1804, CVE-2014-1805, CVE-2014-2753, CVE-2014-2754, CVE-2014-2755, CVE-2014-2756, CVE-2014-2757, CVE-2014-2758, CVE-2014-2759, CVE-2014-2760, CVE-2014-2761, CVE-2014-2763, CVE-2014-2764, CVE-2014-2765, CVE-2014-2766, CVE-2014-2767, CVE-2014-2768, CVE-2014-2769, CVE-2014-2770, CVE-2014-2771, CVE-2014-2772, CVE-2014-2773, CVE-2014-2775, CVE-2014-2776, CVE-2014-2777

Update Details

Recommendation is updated

17205 - GNU Bash Multiple Unspecified Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6277, CVE-2014-6278

Update Details

Recommendation is updated Documentation is updated

17223 - (MS14-057) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4073, CVE-2014-4121, CVE-2014-4122

Update Details

Recommendation is updated

1095 - (MS01-059) Microsoft Windows UPnP NOTIFY Directive Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2001-0876, CVE-2001-0877

Update Details

Recommendation is updated

1598 - (MS03-007) Microsoft IIS WebDAV ntdll.dll Buffer Overflow Intrusive

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2003-0109

Update Details

Recommendation is updated

1782 - (MS03-007) Microsoft Windows ntdll.dll Buffer Overflow Patch Check

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-1999-0744, CVE-2000-0043, CVE-2000-0395, CVE-2000-0484, CVE-2000-0561, CVE-2000-0571, CVE-2003-0109

Update Details

Recommendation is updated

2066 - (MS03-043) Microsoft Windows Messenger Service Buffer Overrun

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2003-0717

Update Details

Recommendation is updated

2081 - (MS03-049) Microsoft Windows Workstation Service Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0812

Update Details

Recommendation is updated

2273 - (MS04-011) Microsoft Windows Security Rollup Patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0533, CVE-2003-0663, CVE-2003-0719, CVE-2003-0806, CVE-2003-0813, CVE-2003-0906, CVE-2003-0907, CVE-2003-0908, CVE-2003-0909, CVE-2003-0910, CVE-2004-0117, CVE-2004-0118, CVE-2004-0119, CVE-2004-0120, CVE-2004-0123, CVE-2005-1935

Update Details

Recommendation is updated

2305 - (MS04-011) Microsoft Windows SSL Library PCT Overrun

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: High

CVE: CVE-2003-0719

Update Details

Recommendation is updated

2561 - (MS04-022) Microsoft Windows Task Scheduler Job Overrun REMOTE

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0212

Update Details

Recommendation is updated

2670 - (MS04-028) Microsoft Windows Buffer Overrun in JPEG Processing (GDI+)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0200

Update Details

Recommendation is updated

2671 - (MS04-028) Microsoft Office Buffer Overrun in JPEG Processing (GDI+)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0200

Update Details

Recommendation is updated

2672 - (MS04-028) Microsoft Internet Explorer Buffer Overrun in JPEG Processing (GDI+)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0200

Update Details

Recommendation is updated

2674 - (MS04-028) Microsoft Visual Studio.NET Overrun in JPEG Processing (GDI+)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0200

Update Details

Recommendation is updated

3130 - (MS05-011) Microsoft Windows SMB Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0045

Update Details

Recommendation is updated

3138 - (MS05-014) Microsoft Internet Explorer Cumulative Security Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0053, CVE-2005-0054, CVE-2005-0055, CVE-2005-0056, CVE-2002-0726

Update Details

Recommendation is updated

3642 - (MS05-043) Microsoft Windows Spooler Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1984

Update Details

Recommendation is updated

3643 - (MS05-038) Microsoft Internet Explorer JPEG Rendering Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1988, CVE-2005-1989, CVE-2005-1990, CVE-2005-2308

Update Details

Recommendation is updated

3645 - (MS05-039) Microsoft Windows SMB PnP Manager Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1983, CVE-2005-1984

Update Details

Recommendation is updated

4360 - (MS06-013) Microsoft Internet Explorer HTA Execution Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1388, CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359

Update Details

Recommendation is updated

4412 - (MS06-024) Microsoft Windows Media Player Vulnerability (917734)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0025

Update Details

Recommendation is updated

4419 - (MS06-032) Microsoft TCP/IP Vulnerability (917953)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2379

Update Details

Recommendation is updated

4428 - (MS06-037) Microsoft Excel Malformed File Vulnerability (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4429 - (MS06-050) Microsoft Windows Hyperlink Object Buffer Overflow (KB920670)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3086, CVE-2006-3438

Update Details

Recommendation is updated

4458 - (MS06-039) Microsoft Office Remote Code Execution Using a Malformed GIF Vulnerability (915384)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0007, CVE-2006-0033

Update Details

Recommendation is updated

4502 - (MS06-050) Microsoft Hyperlink Object Function Vulnerability (KB920670)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3438, CVE-2006-3086

Update Details

Recommendation is updated

4604 - (MS06-054) Microsoft Publisher Vulnerability (910729)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0001

Update Details

Recommendation is updated

4652 - (MS06-058) Microsoft PowerPoint Malformed Record Vulnerability (924163)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3435, CVE-2006-3876, CVE-2006-3877, CVE-2006-4694, CVE-2007-0913

Update Details

Recommendation is updated

4666 - (MS06-063) Microsoft Windows Server Service Denial of Service Vulnerability (923414)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1314, CVE-2006-1315, CVE-2006-3942, CVE-2006-4696

Update Details

Recommendation is updated

4683 - (MS06-063) Microsoft SMB Rename Vulnerability (923414)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1314, CVE-2006-1315, CVE-2006-3942, CVE-2006-4696

Update Details

Recommendation is updated

4698 - (MS05-038) Microsoft Internet Explorer Web Folder Behaviors Cross-Domain

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1988, CVE-2005-1989, CVE-2005-1990, CVE-2005-2308

Update Details

Recommendation is updated

4699 - (MS05-038) Microsoft Internet Explorer COM Instantiation Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1988, CVE-2005-1989, CVE-2005-1990, CVE-2005-2308

Update Details

Recommendation is updated

4709 - (MS05-054) Microsoft Internet Explorer COM Instantiation Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-2831

Update Details

Recommendation is updated

4788 - (MS06-072) Microsoft Script Error Handling Memory Corruption Vulnerability (925454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5577, CVE-2006-5578, CVE-2006-5579, CVE-2006-5581

Update Details

Recommendation is updated

4789 - (MS06-072) Microsoft DHTML Script Function Memory Corruption Vulnerability (925454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5577, CVE-2006-5578, CVE-2006-5579, CVE-2006-5581

Update Details

Recommendation is updated

4790 - (MS06-072) Microsoft TIF Folder Information Disclosure Vulnerability II (925454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5577, CVE-2006-5578, CVE-2006-5579, CVE-2006-5581

Update Details

Recommendation is updated

4791 - (MS06-072) Microsoft TIF Folder Information Disclosure Vulnerability I (925454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5577, CVE-2006-5578, CVE-2006-5579, CVE-2006-5581

Update Details

Recommendation is updated

4792 - (MS06-074) Microsoft SNMP Memory Corruption Vulnerability (926247)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5583

Update Details

Recommendation is updated

4862 - (MS07-001) Microsoft Office 2003 Brazilian Portuguese Grammar Checker Vulnerability (921585)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5574

Update Details

Recommendation is updated

4863 - (MS07-002) Microsoft Excel Malformed IMDATA Record Vulnerability (927198)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031

Update Details

Recommendation is updated

4864 - (MS07-002) Microsoft Excel Malformed Record Vulnerability (927198)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031

Update Details

Recommendation is updated

4865 - (MS07-002) Microsoft Excel Malformed String Vulnerability (927198)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031

Update Details

Recommendation is updated

4866 - (MS07-002) Microsoft Excel Malformed Column Record Vulnerability (927198)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031

Update Details

Recommendation is updated

4867 - (MS07-002) Microsoft Excel Malformed Palette Record Vulnerability (927198)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031

Update Details

Recommendation is updated

4868 - (MS07-003) Microsoft Outlook VEVENT Vulnerability (925938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1305, CVE-2007-0033, CVE-2007-0034

Update Details

Recommendation is updated

4869 - (MS07-003) Microsoft Outlook Denial of Service Vulnerability (925938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1305, CVE-2007-0033, CVE-2007-0034

Update Details

Recommendation is updated

4870 - (MS07-003) Microsoft Outlook Advanced Find Vulnerability (925938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1305, CVE-2007-0033, CVE-2007-0034

Update Details

Recommendation is updated

4871 - (MS07-004) Microsoft VML Buffer Overrun Vulnerability (929969)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0024

Update Details

Recommendation is updated

4907 - (MS07-014) Microsoft Word Malformed Function Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0515

Update Details

Recommendation is updated

4913 - (MS07-015) Microsoft Excel Malformed Record Vulnerability (932554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0671

Update Details

Recommendation is updated

4932 - (MS07-005) Microsoft Interactive Training Vulnerability (923723)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3448

Update Details

Recommendation is updated

4938 - (MS07-012) Microsoft MFC Overrun Vulnerability (924667)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0025

Update Details

Recommendation is updated

4939 - (MS07-013) Microsoft RichEdit Vulnerability (918118)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1311

Update Details

Recommendation is updated

4942 - (MS07-015) Microsoft PowerPoint Malformed Record Memory Corruption Vulnerability (932554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3877, CVE-2007-0671

Update Details

Recommendation is updated

5030 - (MS07-034) Microsoft Windows Mail UNC Navigation Request Remote Code Execution Vulnerability (929123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2111, CVE-2007-1658, CVE-2007-2225, CVE-2007-2227

Update Details

Recommendation is updated

5040 - (MS07-017) Microsoft WMF Denial of Service Vulnerability (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215, CVE-2007-1765

Update Details

Recommendation is updated

5042 - (MS07-017) Microsoft GDI Invalid Window Size Elevation of Privilege Vulnerability (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215, CVE-2007-1765

Update Details

Recommendation is updated

5043 - (MS07-017) GDI Incorrect Parameter Local Elevation of Privilege Vulnerability (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1215, CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1765

Update Details

Recommendation is updated

5044 - (MS07-017) Microsoft Font Rasterizer Vulnerability (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215, CVE-2007-1765

Update Details

Recommendation is updated

5060 - (MS07-020) Microsoft Agent URL Parsing Vulnerability (932168)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1205

Update Details

Recommendation is updated

5075 - (MS07-029) Microsoft DNS RPC Management Vulnerability (935966)

Category: General Vulnerability Assessment -> Instrusive -> Windows

Risk Level: High

CVE: CVE-2007-1748

Update Details

Recommendation is updated

5076 - (MS07-029) Microsoft DNS RPC Management Vulnerability (935966)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1748

Update Details

Recommendation is updated

5125 - (MS07-024) Microsoft Word Array Overflow (934232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0035, CVE-2007-0870, CVE-2007-1202

Update Details

Recommendation is updated

5126 - (MS07-025) Microsoft Office Drawing Object Vulnerability (934873)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1747

Update Details

Recommendation is updated

5131 - (MS07-027) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (931768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0944, CVE-2007-0323, CVE-2007-0942, CVE-2007-0945, CVE-2007-0946, CVE-2007-0947, CVE-2007-2221

Update Details

Recommendation is updated

5132 - (MS07-027) Microsoft Internet Explorer Property Memory Corruption Vulnerability (931768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0945, CVE-2007-0323, CVE-2007-0942, CVE-2007-0944, CVE-2007-0946, CVE-2007-0947, CVE-2007-2221

Update Details

Recommendation is updated

5133 - (MS07-027) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability I (931768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0946, CVE-2007-0323, CVE-2007-0942, CVE-2007-0944, CVE-2007-0945, CVE-2007-0947, CVE-2007-2221

Update Details

Recommendation is updated

5134 - (MS07-027) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability II (931768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0947, CVE-2007-0323, CVE-2007-0942, CVE-2007-0944, CVE-2007-0945, CVE-2007-0946, CVE-2007-2221

Update Details

Recommendation is updated

5135 - (MS07-027) Microsoft Internet Explorer Arbitrary File Rewrite Vulnerability (931768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0323, CVE-2007-0942, CVE-2007-0944, CVE-2007-0945, CVE-2007-0946, CVE-2007-0947, CVE-2007-2221

Update Details

Recommendation is updated

5138 - (MS07-027) Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability (931768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0942, CVE-2007-0323, CVE-2007-0944, CVE-2007-0945, CVE-2007-0946, CVE-2007-0947, CVE-2007-2221

Update Details

Recommendation is updated

5139 - (MS07-028) Microsoft CAPICOM Certificates Vulnerability (931906)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0940

Update Details

Recommendation is updated

5224 - (MS07-030) Microsoft Visio Version Number Memory Corruption Vulnerability (927051)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0934, CVE-2007-0936

Update Details

Recommendation is updated

5225 - (MS07-030) Microsoft Visio Document Packaging Vulnerability (927051)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0936, CVE-2007-0934

Update Details

Recommendation is updated

5228 - (MS07-033) Microsoft COM Object Instantiation Memory Corruption Vulnerability (933566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0218, CVE-2007-1499, CVE-2007-1750, CVE-2007-1751, CVE-2007-1752, CVE-2007-2222, CVE-2007-3027

Update Details

Recommendation is updated

5229 - (MS07-033) Microsoft CSS Tag Memory Corruption Vulnerability (933566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0218, CVE-2007-1499, CVE-2007-1750, CVE-2007-1751, CVE-2007-1752, CVE-2007-2222, CVE-2007-3027

Update Details

Recommendation is updated

5231 - (MS07-033) Microsoft Uninitialized Memory Corruption Vulnerability (933566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0218, CVE-2007-1499, CVE-2007-1750, CVE-2007-1751, CVE-2007-1752, CVE-2007-2222, CVE-2007-3027

Update Details

Recommendation is updated

5232 - (MS07-033) Microsoft Speech Control Memory Corruption Vulnerability (933566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0218, CVE-2007-1499, CVE-2007-1750, CVE-2007-1751, CVE-2007-1752, CVE-2007-2222, CVE-2007-3027

Update Details

Recommendation is updated

5233 - (MS07-034) Microsoft URL Redirect Cross Domain Information Disclosure Vulnerability (929123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2111, CVE-2007-1658, CVE-2007-2225, CVE-2007-2227

Update Details

Recommendation is updated

5234 - (MS07-034) Microsoft URL Parsing Cross Domain Information Disclosure Vulnerability (929123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2111, CVE-2007-1658, CVE-2007-2225, CVE-2007-2227

Update Details

Recommendation is updated

5235 - (MS07-034) Microsoft Content Disposition Parsing Cross Domain Information Disclosure Vulnerability (929123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2111, CVE-2007-1658, CVE-2007-2225, CVE-2007-2227

Update Details

Recommendation is updated

5321 - (MS07-040) Microsoft .NET PE Loader Vulnerability (931212)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0041, CVE-2007-0042, CVE-2007-0043

Update Details

Recommendation is updated

5322 - (MS07-040) Microsoft ASP.NET Null Byte Termination Vulnerability (931212)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0041, CVE-2007-0042, CVE-2007-0043

Update Details

Recommendation is updated

5323 - (MS07-040) Microsoft .NET JIT Compiler Vulnerability (931212)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0041, CVE-2007-0042, CVE-2007-0043

Update Details

Recommendation is updated

5325 - (MS07-036) Microsoft Excel Calculation Error Vulnerability (936542)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1756, CVE-2007-3029, CVE-2007-3030

Update Details

Recommendation is updated

5326 - (MS07-036) Microsoft Excel Worksheet Memory Corruption Vulnerability (936542)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1756, CVE-2007-3029, CVE-2007-3030

Update Details

Recommendation is updated

5327 - (MS07-036) Microsoft Excel Workbook Memory Corruption (936542)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1756, CVE-2007-3029, CVE-2007-3030

Update Details

Recommendation is updated

5354 - (MS07-057) Microsoft Internet Explorer Address Bar Spoofing Vulnerability III (939653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3826

Update Details

Recommendation is updated

5414 - (MS07-043) Microsoft OLE Automation Memory Corruption Vulnerability (921503)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2224

Update Details

Recommendation is updated

5415 - (MS07-045) Microsoft Internet Explorer CSS Memory Corruption Vulnerability (937143)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0943, CVE-2007-2216, CVE-2007-3041

Update Details

Recommendation is updated

5416 - (MS07-045) Microsoft Internet Explorer ActiveX Object Vulnerability (937143)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0943, CVE-2007-2216, CVE-2007-3041

Update Details

Recommendation is updated

5417 - (MS07-045) Microsoft Internet Explorer ActiveX Object Memory Corruption Vulnerability (937143)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0943, CVE-2007-2216, CVE-2007-3041

Update Details

Recommendation is updated

5418 - (MS07-046) Microsoft Remote Code Execution Vulnerability in GDI (938829)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3034

Update Details

Recommendation is updated

5421 - (MS07-049) Microsoft Virtual PC Heap Overflow Vulnerability (937986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0948

Update Details

Recommendation is updated

5423 - (MS07-044) Microsoft Excel Workspace Memory Corruption Vulnerability (940965)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3890

Update Details

Recommendation is updated

5426 - (MS07-049) Microsoft Virtual Server Heap Overflow Vulnerability (937986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0948

Update Details

Recommendation is updated

5480 - (MS07-051) Microsoft Agent Remote Code Execution Vulnerability (938827)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3040

Update Details

Recommendation is updated

5514 - (MS07-055) Microsoft Windows Kodak Image Viewer Remote Code Execution Vulnerability (923810)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2217

Update Details

Recommendation is updated

5516 - (MS07-057) Microsoft Internet Explorer Address Bar Spoofing Vulnerability I (939653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1091, CVE-2007-3826, CVE-2007-3892, CVE-2007-3893

Update Details

Recommendation is updated

5518 - (MS07-056) Microsoft Network News Transfer Protocol Memory Corruption Vulnerability (941202)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3897

Update Details

Recommendation is updated

5520 - (MS07-057) Microsoft Internet Explorer Address Bar Spoofing Vulnerability II (939653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1091, CVE-2007-3826, CVE-2007-3892, CVE-2007-3893

Update Details

Recommendation is updated

5521 - (MS07-060) Microsoft Word Memory Corruption Vulnerability (942695)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3899

Update Details

Recommendation is updated

5531 - (MS07-061) Microsoft Windows URI Handling Vulnerability (943460)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3896

Update Details

Recommendation is updated

5602 - (MS08-028) Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability (950749)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-6026, CVE-2007-6357, CVE-2008-1200, CVE-2008-1092

Update Details

Recommendation is updated

5623 - (MS07-064) Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files (941568)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3895, CVE-2007-3901

Update Details

Recommendation is updated

5624 - (MS07-064) Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files (941568)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3901, CVE-2007-3895

Update Details

Recommendation is updated

5625 - (MS07-065) Microsoft Message Queuing Service Remote Code Execution Vulnerability (937894)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3039

Update Details

Recommendation is updated

5627 - (MS07-068) Microsoft Windows Media Format Remote Code Execution Vulnerability Parsing ASF (941569)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0064

Update Details

Recommendation is updated

5628 - (MS07-069) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability I (942615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3902, CVE-2007-3903, CVE-2007-5344, CVE-2007-5347

Update Details

Recommendation is updated

5629 - (MS07-069) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability II (942615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3902, CVE-2007-3903, CVE-2007-5344, CVE-2007-5347

Update Details

Recommendation is updated

5630 - (MS07-069) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability III(942615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3902, CVE-2007-3903, CVE-2007-5344, CVE-2007-5347

Update Details

Recommendation is updated

5631 - (MS07-069) Microsoft Internet Explorer DHTML Objects Memory Corruption Vulnerabilities (942615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3902, CVE-2007-3903, CVE-2007-5344, CVE-2007-5347

Update Details

Recommendation is updated

5652 - (MS08-001) Microsoft Windows Kernel TCP/IP/IGMPv3 and MLDv2 Vulnerability (941644)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0066, CVE-2007-0069

Update Details

Recommendation is updated

5653 - (MS08-001) Microsoft Windows Kernel TCP/IP/ICMP Vulnerability (941644)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0066, CVE-2007-0069

Update Details

Recommendation is updated

5674 - (MS08-014) Microsoft Macro Validation Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081 , CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5701 - (MS08-010) Microsoft HTML Rendering Memory Corruption Vulnerability (944533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-4790, CVE-2008-0076, CVE-2008-0077, CVE-2008-0078

Update Details

Recommendation is updated

5702 - (MS08-010) Microsoft Property Memory Corruption Vulnerability (944533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-4790, CVE-2008-0076, CVE-2008-0077, CVE-2008-0078

Update Details

Recommendation is updated

5703 - (MS08-010) Microsoft Argument Handling Memory Corruption Vulnerability (944533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-4790, CVE-2008-0076, CVE-2008-0077, CVE-2008-0078

Update Details

Recommendation is updated

5704 - (MS08-010) Microsoft ActiveX Object Memory Corruption Vulnerability (944533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-4790, CVE-2008-0076, CVE-2008-0077, CVE-2008-0078

Update Details

Recommendation is updated

5705 - (MS08-011) Microsoft Works Converter Input Validation Vulnerability (947081)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0216, CVE-2008-0105, CVE-2008-0108

Update Details

Recommendation is updated

5706 - (MS08-011) Microsoft Works Converter Index Table Vulnerability (947081)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0105, CVE-2007-0216, CVE-2008-0108

Update Details

Recommendation is updated

5707 - (MS08-011) Microsoft Works File Converter Field Length Vulnerability (947081)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0108, CVE-2007-0216, CVE-2008-0105

Update Details

Recommendation is updated

5712 - (MS08-009) Microsoft Word Memory Corruption Vulnerability (947077)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0109

Update Details

Recommendation is updated

5741 - (MS08-017) Microsoft Office Web Components URL Parsing Vulnerability (933103)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4695, CVE-2007-1201

Update Details

Recommendation is updated

5742 - (MS08-017) Microsoft Office Web Components DataSource Vulnerability (933103)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4695, CVE-2007-1201

Update Details

Recommendation is updated

5743 - (MS08-014) Microsoft Excel Data Validation Record Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5744 - (MS08-014) Microsoft Excel File Import Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5745 - (MS08-014) Microsoft Excel Style Record Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5746 - (MS08-014) Microsoft Excel Formula Parsing Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5747 - (MS08-014) Microsoft Excel Rich Text Validation Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5748 - (MS08-014) Microsoft Excel Conditional Formatting Vulnerability (949029)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117

Update Details

Recommendation is updated

5749 - (MS08-016) Microsoft Office Cell Parsing Memory Corruption Vulnerability (949030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0113, CVE-2008-0118

Update Details

Recommendation is updated

5750 - (MS08-016) Microsoft Office Memory Corruption Vulnerability (949030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0113, CVE-2008-0118

Update Details

Recommendation is updated

5751 - (MS08-015) Microsoft Outlook URI Vulnerability (949031)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0110

Update Details

Recommendation is updated

5806 - (MS08-024) Microsoft Data Stream Handling Memory Corruption Vulnerability (947864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1085

Update Details

Recommendation is updated

5808 - (MS08-022) Microsoft VBScript and JScript Remote Code Execution Vulnerability (944338)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0083

Update Details

Recommendation is updated

5810 - (MS08-021) Microsoft GDI Heap Overflow Vulnerability (948590)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1083, CVE-2008-1087

Update Details

Recommendation is updated

5812 - (MS08-019) Microsoft Visio Memory Validation Vulnerability (949032)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1089, CVE-2008-1090

Update Details

Recommendation is updated

5813 - (MS08-019) Microsoft Visio Object Header Vulnerability (949032)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1089, CVE-2008-1090

Update Details

Recommendation is updated

5814 - (MS08-018) Microsoft Project Memory Validation Vulnerability (950183)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1088

Update Details

Recommendation is updated

5862 - (MS08-026) Microsoft Object Parsing Vulnerability (951207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1091, CVE-2008-1434

Update Details

Recommendation is updated

5863 - (MS08-026) Microsoft Word Cascading Style Sheet (CSS) Vulnerability (951207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1091, CVE-2008-1434

Update Details

Recommendation is updated

5864 - (MS08-027) Microsoft Publisher Object Handler Validation Vulnerability (951208)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0119

Update Details

Recommendation is updated

5920 - (MS08-031) Microsoft HTML Objects Memory Corruption Vulnerability (950759)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1442, CVE-2008-1544

Update Details

Recommendation is updated

5921 - (MS08-031) Microsoft Request Header Cross-Domain Information Disclosure Vulnerability (950759)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1442, CVE-2008-1544

Update Details

Recommendation is updated

5923 - (MS08-033) Microsoft MJPEG Decoder Vulnerability (951698)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0011, CVE-2008-1444

Update Details

Recommendation is updated

5924 - (MS08-033) Microsoft SAMI Format Parsing Vulnerability (951698)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1444, CVE-2008-0011

Update Details

Recommendation is updated

5987 - (MS08-037) Microsoft DNS Cache Poisoning Vulnerability (953230)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1447, CVE-2008-1454

Update Details

Recommendation is updated

5988 - (MS08-038) Microsoft Windows Saved Search Vulnerability (950582)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1435

Update Details

Recommendation is updated

5991 - (MS08-040) Microsoft Memory Page Reuse Vulnerability (941203)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0085, CVE-2008-0086, CVE-2008-0106, CVE-2008-0107

Update Details

Recommendation is updated

5992 - (MS08-040) Microsoft Convert Buffer Overrun Vulnerability (941203)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0085, CVE-2008-0086, CVE-2008-0106, CVE-2008-0107

Update Details

Recommendation is updated

5993 - (MS08-040) Microsoft SQL Memory Corruption Vulnerability (941203)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0085, CVE-2008-0086, CVE-2008-0106, CVE-2008-0107

Update Details

Recommendation is updated

5994 - (MS08-040) Microsoft SQL Buffer Overrun Vulnerability (941203)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0085, CVE-2008-0086, CVE-2008-0106, CVE-2008-0107

Update Details

Recommendation is updated

5999 - (MS08-042) Microsoft Word Record Parsing Vulnerability (955048)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2244

Update Details

Recommendation is updated

6043 - (MS08-043) Microsoft Excel Indexing Validation Vulnerability (954066)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3003, CVE-2008-3004 , CVE-2008-3005, CVE-2008-3006

Update Details

Recommendation is updated

6044 - (MS08-043) Microsoft Excel Index Array Vulnerability (954066)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3003, CVE-2008-3004, CVE-2008-3005, CVE-2008-3006

Update Details

Recommendation is updated

6045 - (MS08-043) Microsoft Excel Record Parsing Vulnerability (954066)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3003, CVE-2008-3004, CVE-2008-3005, CVE-2008-3006

Update Details

Recommendation is updated

6046 - (MS08-043) Microsoft Excel Credential Caching Vulnerability (954066)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3003 , CVE-2008-3004, CVE-2008-3005, CVE-2008-3006

Update Details

Recommendation is updated

6047 - (MS08-044) Microsoft Malformed EPS Filter Vulnerability (924090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3018, CVE-2008-3019 , CVE-2008-3020, CVE-2008-3021, CVE-2008-3460

Update Details

Recommendation is updated

6048 - (MS08-044) Microsoft Malformed PICT Filter Vulnerability (924090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3018 , CVE-2008-3019, CVE-2008-3020, CVE-2008-3021, CVE-2008-3460

Update Details

Recommendation is updated

6049 - (MS08-044) Microsoft PICT Filter Parsing Vulnerability (924090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3018, CVE-2008-3019, CVE-2008-3020, CVE-2008-3021 , CVE-2008-3460

Update Details

Recommendation is updated

6050 - (MS08-044) Microsoft Malformed BMP Filter Vulnerability (924090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3018, CVE-2008-3019, CVE-2008-3020 , CVE-2008-3021, CVE-2008-3460

Update Details

Recommendation is updated

6051 - (MS08-044) Microsoft Office WPG Image File Heap Corruption Vulnerability (924090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3018, CVE-2008-3019, CVE-2008-3020, CVE-2008-3021, CVE-2008-3460

Update Details

Recommendation is updated

6052 - (MS08-045) Microsoft HTML Objects Memory Corruption Vulnerability I (953838)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2258, CVE-2008-2254, CVE-2008-2255, CVE-2008-2256, CVE-2008-2257, CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

6053 - (MS08-045) Microsoft HTML Objects Memory Corruption Vulnerability II (953838)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2258, CVE-2008-2254, CVE-2008-2255 , CVE-2008-2256, CVE-2008-2257, CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

6054 - (MS08-045) Microsoft Uninitialized Memory Corruption Vulnerability (953838)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2258, CVE-2008-2254, CVE-2008-2255, CVE-2008-2256, CVE-2008-2257, CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

6055 - (MS08-045) Microsoft HTML Objects Memory Corruption Vulnerability III (953838)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2258, CVE-2008-2254, CVE-2008-2255, CVE-2008-2256, CVE-2008-2257 , CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

6056 - (MS08-045) Microsoft HTML Objects Memory Corruption Vulnerability IV (953838)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2258, CVE-2008-2254, CVE-2008-2255, CVE-2008-2256, CVE-2008-2257, CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

6057 - (MS08-045) Microsoft Component Handling Memory Corruption Vulnerability (953838)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2258, CVE-2008-2254, CVE-2008-2255, CVE-2008-2256, CVE-2008-2257, CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

6058 - (MS08-046) Microsoft Color Management System Vulnerability (952954)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2245

Update Details

Recommendation is updated

6061 - (MS08-049) Microsoft Event System Vulnerability I (950974)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1457 , CVE-2008-1456

Update Details

Recommendation is updated

6062 - (MS08-049) Microsoft Event System Vulnerability II (950974)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1456 , CVE-2008-1457

Update Details

Recommendation is updated

6064 - (MS08-051) Microsoft Memory Allocation Vulnerability (949785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0120 , CVE-2008-0121, CVE-2008-1455

Update Details

Recommendation is updated

6065 - (MS08-051) Microsoft Memory Calculation Vulnerability (949785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0120, CVE-2008-0121 , CVE-2008-1455

Update Details

Recommendation is updated

6066 - (MS08-051) Microsoft Parsing Overflow Vulnerability (949785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0120, CVE-2008-0121, CVE-2008-1455

Update Details

Recommendation is updated

6080 - (MS03-051) Microsoft FrontPage Server Extensions Buffer Overflow

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2003-0822, CVE-2003-0824

Update Details

Recommendation is updated

6104 - (MS08-055) Microsoft Uniform Resource Locator Validation Error Vulnerability (955047)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3007

Update Details

Recommendation is updated

6105 - (MS08-052) Microsoft GDI+ VML Buffer Overrun Vulnerability (954593)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6106 - (MS08-052) Microsoft GDI+ EMF Memory Corruption Vulnerability (954593)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6107 - (MS08-052) Microsoft GDI+ GIF Parsing Vulnerability (954593)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6108 - (MS08-052) Microsoft GDI+WMF Buffer Overrun Vulnerability (954593)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6109 - (MS08-052) Microsoft GDI+ BMP Integer Overflow Vulnerability (954593)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6110 - (MS08-053) Microsoft Windows Media Encoder Remote Code Execution (954156)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3008

Update Details

Recommendation is updated

6111 - (MS08-054) Microsoft Windows Media Player Sampling Rate Vulnerability (954154)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2253

Update Details

Recommendation is updated

6153 - (MS09-012) Microsoft Windows MSDTC Service Isolation Vulnerability (959454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1436

Update Details

Recommendation is updated

6168 - (MS08-062) Microsoft Integer Overflow in IPP Service Vulnerability (953155)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1446

Update Details

Recommendation is updated

6172 - (MS08-058) Microsoft HTML Tag Element Cross-Domain Information Disclosure Vulnerability (956390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3472

Update Details

Recommendation is updated

6173 - (MS08-058) Microsoft Source Element Cross-Domain Information Disclosure Vulnerability (956390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3473

Update Details

Recommendation is updated

6175 - (MS08-058) Microsoft Uninitialized Memory Corruption Vulnerability (956390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3475

Update Details

Recommendation is updated

6176 - (MS08-058) Microsoft HTML Objects Memory Corruption Vulnerability (956390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3476

Update Details

Recommendation is updated

6177 - (MS08-058) Microsoft Internet Explorer CPeerHolder::CPeerSite::QueryService() Vulnerability (KB956390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3472

Update Details

Recommendation is updated

6217 - (MS08-069) Microsoft MSXML Nested Tag Vulnerability (955218)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0099

Update Details

Recommendation is updated

6220 - (MS08-068) Microsoft SMB Credential Reflection Vulnerability (957097)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4037

Update Details

Recommendation is updated

6267 - (MS08-070) Microsoft DataGrid Control Memory Corruption Vulnerability (932349)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4252

Update Details

Recommendation is updated

6270 - (MS08-070) Microsoft Masked Edit Control Memory Corruption Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3704

Update Details

Recommendation is updated

6271 - (MS08-070) Microsoft Windows Common AVI Parsing Overflow Vulnerability (932349)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4255

Update Details

Recommendation is updated

6273 - (MS08-071) Microsoft GDI Heap Overflow Vulnerability (956802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3465

Update Details

Recommendation is updated

6274 - (MS08-071) Microsoft GDI Integer Overflow Vulnerability (956802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2249

Update Details

Recommendation is updated

6283 - (MS08-073) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability (958215)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4259

Update Details

Recommendation is updated

6284 - (MS08-073) Microsoft Internet Explorer HTML Rendering Memory Corruption Vulnerability (958215)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4261

Update Details

Recommendation is updated

6287 - (MS08-074) Microsoft Excel File Format Parsing Vulnerability I (959070)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4265

Update Details

Recommendation is updated

6288 - (MS08-074) Microsoft Excel File Format Parsing Vulnerability II (959070)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4264

Update Details

Recommendation is updated

6289 - (MS08-074) Microsoft Excel Global Array Memory Corruption Vulnerability (959070)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4266

Update Details

Recommendation is updated

6290 - (MS08-075) Microsoft Windows Saved Search Vulnerability (959349)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4268

Update Details

Recommendation is updated

6300 - (MS09-010) Microsoft WordPad Word 97 Text Converter Stack Overflow Vulnerability (960477)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4841

Update Details

Recommendation is updated

6315 - (MS09-004) Microsoft SQL Server sp_replwritetovarbin Limited Memory Overwrite Vulnerability (959420)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-5416

Update Details

Recommendation is updated

6420 - (MS09-005) Microsoft Visio Memory Corruption Vulnerability - CVE-2009-0096 - (957634)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0096

Update Details

Recommendation is updated

6421 - (MS09-005) Microsoft Visio Memory Corruption Vulnerability - CVE-2009-0097 - (957634)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0097

Update Details

Recommendation is updated

6422 - (MS09-003) Microsoft Exchange Memory Corruption Vulnerability (959239)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0098

Update Details

Recommendation is updated

6583 - (MS09-017) Microsoft PowerPoint Memory Corruption Vulnerability II (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0556

Update Details

Recommendation is updated

6596 - (MS09-010) Microsoft Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability (960477)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0088

Update Details

Recommendation is updated

6597 - (MS09-010) Microsoft WordPad and Office Text Converter Memory Corruption Vulnerability (960477)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0087

Update Details

Recommendation is updated

6598 - (MS09-010) Microsoft WordPad Word 97 Text Converter Stack Overflow Vulnerability II (960477)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0235

Update Details

Recommendation is updated

6599 - (MS09-011) Microsoft MJPEG Decompression Vulnerability (961373)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0084

Update Details

Recommendation is updated

6604 - (MS09-013) Microsoft Windows HTTP Services Credential Reflection Vulnerability (960803)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0550

Update Details

Recommendation is updated

6606 - (MS09-014) Microsoft Internet Explorer Page Transition Memory Corruption Vulnerability (963027)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0551

Update Details

Recommendation is updated

6610 - (MS09-014) Microsoft Internet Explorer WinINet Remote Code Execution vulnerability (963027)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0550

Update Details

Recommendation is updated

6611 - (MS09-015) Microsoft Windows Blended Threat Elevation of Privilege Vulnerability (959426)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2540

Update Details

Recommendation is updated

6662 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0220

Update Details

Recommendation is updated

6663 - (MS09-017) Microsoft PowerPoint Integer Overflow Vulnerability (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0221

Update Details

Recommendation is updated

6664 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability II (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0222

Update Details

Recommendation is updated

6665 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability III (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0223

Update Details

Recommendation is updated

6666 - (MS09-017) Microsoft PowerPoint Memory Corruption Vulnerability (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0224

Update Details

Recommendation is updated

6667 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability IV (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0225

Update Details

Recommendation is updated

6668 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability V (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0226

Update Details

Recommendation is updated

6669 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability VI (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0227

Update Details

Recommendation is updated

6670 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability VII (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1128

Update Details

Recommendation is updated

6671 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability VIII (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1129

Update Details

Recommendation is updated

6672 - (MS09-017) Microsoft PowerPoint Heap Corruption Vulnerability (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1130

Update Details

Recommendation is updated

6673 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability IX (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1137

Update Details

Recommendation is updated

6674 - (MS09-017) Microsoft PowerPoint Data Out of Bounds Vulnerability (967340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1131

Update Details

Recommendation is updated

6717 - (MS09-028) Microsoft DirectShow DirectX NULL Byte Overwrite Vulnerability (971633)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1537

Update Details

Recommendation is updated

6745 - (MS09-019) Microsoft Internet Explorer DHTML Object Memory Corruption Vulnerability (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1141

Update Details

Recommendation is updated

6746 - (MS09-019) Microsoft Internet Explorer HTML Object Memory Corruption (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1528

Update Details

Recommendation is updated

6747 - (MS09-019) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1530

Update Details

Recommendation is updated

6748 - (MS09-019) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability II (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1531

Update Details

Recommendation is updated

6749 - (MS09-019) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability III (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1532

Update Details

Recommendation is updated

6751 - (MS09-019) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1529

Update Details

Recommendation is updated

6759 - (MS09-021) Microsoft Office Excel Record Pointer Corruption Vulnerability II (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1134

Update Details

Recommendation is updated

6762 - (MS09-022) Microsoft Windows Print Spooler Load Library Vulnerability (961501)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0230

Update Details

Recommendation is updated

6765 - (MS09-024) Microsoft Works File Converter Buffer Overflow Vulnerability (957632)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1533

Update Details

Recommendation is updated

6835 - (MS09-043) Microsoft Office Web Components HTML Script Vulnerability (957638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1136

Update Details

Recommendation is updated

6837 - (MS09-028) Microsoft DirectShow DirectX Pointer Validation Vulnerability (971633)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1538

Update Details

Recommendation is updated

6838 - (MS09-028) Microsoft DirectShow DirectX Size Validation Vulnerability (971633)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1539

Update Details

Recommendation is updated

6839 - (MS09-029) Microsoft Windows Embedded OpenType Font Heap Overflow Vulnerability (961371)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0231

Update Details

Recommendation is updated

6840 - (MS09-029) Microsoft Windows Embedded OpenType Font Integer Overflow Vulnerability (961371)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0232

Update Details

Recommendation is updated

6841 - (MS09-030) Microsoft Publisher Pointer Dereference Vulnerability (969516)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0566

Update Details

Recommendation is updated

6842 - (MS09-031) Microsoft ISA Server Radius OTP Bypass Vulnerability (970811)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1135

Update Details

Recommendation is updated

6844 - (MS09-033) Microsoft Virtual PC and Virtual Server Privileged Instruction Decoding Vulnerability (969856)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1542

Update Details

Recommendation is updated

6901 - (MS09-035) ATL Uninitialized Object Vulnerability (969706)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0901

Update Details

Recommendation is updated

6902 - (MS09-035) ATL COM Initialization Vulnerability (969706)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2493

Update Details

Recommendation is updated

6904 - (MS09-034) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (972260)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1919

Update Details

Recommendation is updated

6905 - (MS09-034) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability (972260)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1918

Update Details

Recommendation is updated

6906 - (MS09-034) Microsoft Internet Explorer Memory Corruption Vulnerability (972260)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1917

Update Details

Recommendation is updated

6952 - (MS09-043) Microsoft Office Web Components Memory Allocation Vulnerability (957638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0562

Update Details

Recommendation is updated

6953 - (MS09-043) Microsoft Office Web Components Heap Corruption Vulnerability (957638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2496

Update Details

Recommendation is updated

6955 - (MS09-043) Microsoft Office Web Components Buffer Overflow Vulnerability (967638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1534

Update Details

Recommendation is updated

6956 - (MS09-037) Microsoft ATL COM Initialization Vulnerability (973908)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2493

Update Details

Recommendation is updated

6957 - (MS09-037) Microsoft ATL Header Memcopy Vulnerability (973908)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0020

Update Details

Recommendation is updated

6959 - (MS09-037) Microsoft ATL Uninitialized Object Vulnerability (973908)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0901

Update Details

Recommendation is updated

6960 - (MS09-037) Microsoft Video ActiveX Control Vulnerability (973908)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0015

Update Details

Recommendation is updated

6963 - (MS09-039) Microsoft WINS Heap Overflow Vulnerability (969883)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1923

Update Details

Recommendation is updated

6964 - (MS09-039) Microsoft WINS Integer Overflow Vulnerability (969883)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1924

Update Details

Recommendation is updated

6966 - (MS09-041) Microsoft Workstation Service Memory Corruption Vulnerability (971657)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1544

Update Details

Recommendation is updated

6968 - (MS09-044) Microsoft Remote Desktop Connection ActiveX Control Heap Overflow Vulnerability (970927)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1929

Update Details

Recommendation is updated

6969 - (MS09-044) Microsoft Remote Desktop Connection Heap Overflow Vulnerability (970927)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1133

Update Details

Recommendation is updated

7098 - (MS09-045) Microsoft Windows Jscript Remote Code Execution Vulnerability (971961)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1920

Update Details

Recommendation is updated

7104 - (MS09-053) IIS FTP Service RCE and Denial of Service Vulnerability (975254)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3023

Update Details

Recommendation is updated

7110 - (MS09-049) Microsoft Windows Wireless Frame Parsing Remote Code Execution Vulnerability (970710)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1132

Update Details

Recommendation is updated

7137 - (MS09-039) Microsoft WINS Heap Overflow Vulnerability (969883)

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2009-1923

Update Details

Recommendation is updated

7172 - (MS09-045) Vulnerability In JScript Scripting Engine Could Allow Remote Code Execution (971961)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1920

Update Details

Recommendation is updated

7176 - (MS09-049) Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1132

Update Details

Recommendation is updated

7190 - (MS09-051) Windows Media Runtime Heap Corruption Vulnerability (975682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2525

Update Details

Recommendation is updated

7191 - (MS09-051) Windows Media Runtime Voice Sample Rate Vulnerability (975682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0555

Update Details

Recommendation is updated

7192 - (MS09-052) WMP Heap Overflow Vulnerability (974112)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2527

Update Details

Recommendation is updated

7194 - (MS09-054) Data Stream Header Corruption Vulnerability (974455)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1547

Update Details

Recommendation is updated

7195 - (MS09-054) Uninitialized Memory Corruption Vulnerability (974455)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2530

Update Details

Recommendation is updated

7201 - (MS09-057) Memory Corruption in Indexing Service Vulnerability (969059)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2507

Update Details

Recommendation is updated

7206 - (MS09-060) ATL COM Initialization Vulnerability (973965)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2493

Update Details

Recommendation is updated

7207 - (MS09-060) ATL Uninitialized Object Vulnerability (973965)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0901

Update Details

Recommendation is updated

7208 - (MS09-061) Microsoft .NET Framework CAS Pointer Verification Vulnerability (974378)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0090

Update Details

Recommendation is updated

7209 - (MS09-061) Microsoft .NET Framework CAS Type Verification Vulnerability II (974378)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0091

Update Details

Recommendation is updated

7210 - (MS09-061) Silverlight and Microsoft .NET Framework CLR Vulnerability (974378)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2497

Update Details

Recommendation is updated

7211 - (MS09-062) GDI+ .Net PropertyItem Heap Overflow Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2504

Update Details

Recommendation is updated

7212 - (MS09-062) GDI+ PNG Heap Overflow Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2501

Update Details

Recommendation is updated

7213 - (MS09-062) GDI+ PNG Integer Overflow Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3126

Update Details

Recommendation is updated

7214 - (MS09-062) GDI+ TIFF Memory Corruption Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2503

Update Details

Recommendation is updated

7215 - (MS09-062) GDI+ TIFF Buffer Overflow Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2502

Update Details

Recommendation is updated

7216 - (MS09-062) GDI+ WMF Integer Overflow Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2500

Update Details

Recommendation is updated

7217 - (MS09-062) Memory Corruption Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2528

Update Details

Recommendation is updated

7218 - (MS09-062) Office BMP Integer Overflow Vulnerability (957488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2518

Update Details

Recommendation is updated

7230 - (MS09-057) Vulnerability In Indexing Service Could Allow Remote Code Execution (969059)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2507

Update Details

Recommendation is updated

7315 - (MS09-068) Vulnerability in Microsoft Office Word Allows Remote Code Execution (976307)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3135

Update Details

Recommendation is updated

7318 - (MS09-065) Win32k EOT Parsing Vulnerability (969947)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2514

Update Details

Recommendation is updated

7319 - (MS09-067) Excel Cache Memory Corruption Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3127

Update Details

Recommendation is updated

7320 - (MS09-067) Excel SxView Memory Corruption Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3128

Update Details

Recommendation is updated

7321 - (MS09-067) Excel Featheader Record Memory Corruption Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3129

Update Details

Recommendation is updated

7322 - (MS09-067) Excel Document Parsing Heap Overflow Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3130

Update Details

Recommendation is updated

7323 - (MS09-067) Excel Formula Parsing Memory Corruption Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3131

Update Details

Recommendation is updated

7324 - (MS09-067) Excel Index Parsing Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3132

Update Details

Recommendation is updated

7325 - (MS09-067) Excel Document Parsing Memory Corruption Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3133

Update Details

Recommendation is updated

7326 - (MS09-067) Excel Field Sanitization Vulnerability (972652)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3134

Update Details

Recommendation is updated

7330 - (MS09-063) Vulnerability In Web Services On Devices API Could Allow Remote Code Execution (973565)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2512

Update Details

Recommendation is updated

7334 - (MS09-067) Vulnerabilities In Microsoft Office Excel Could Allow Remote Code Execution (972652)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3127, CVE-2009-3128, CVE-2009-3129, CVE-2009-3130, CVE-2009-3131, CVE-2009-3132, CVE-2009-3133, CVE-2009-3134

Update Details

Recommendation is updated

7335 - (MS09-068) Vulnerability In Microsoft Office Word Could Allow Remote Code Execution (976307)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3135

Update Details

Recommendation is updated

7344 - (MS09-012) Vulnerabilities In Windows Could Allow Elevation Of Privilege (959454)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1436, CVE-2009-0078, CVE-2009-0079, CVE-2009-0080

Update Details

Recommendation is updated

7345 - (MS09-013) Vulnerabilities In Windows HTTP Services Could Allow Remote Code Execution (960803)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0086, CVE-2009-0089, CVE-2009-0550

Update Details

Recommendation is updated

7347 - (MS09-015) Blended Threat Vulnerability In SearchPath Could Allow Elevation Of Privilege (959426)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2540

Update Details

Recommendation is updated

7356 - (MS09-017) Vulnerabilities In Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0220, CVE-2009-0221, CVE-2009-0222, CVE-2009-0223, CVE-2009-0224, CVE-2009-0225, CVE-2009-0226, CVE-2009-0227, CVE-2009-0556, CVE-2009-1128, CVE-2009-1129, CVE-2009-1130, CVE-2009-1131, CVE-2009-1137

Update Details

Recommendation is updated

7365 - (MS09-003) Vulnerabilities In Microsoft Exchange Could Allow Remote Code Execution (959239)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0098, CVE-2009-0099

Update Details

Recommendation is updated

7366 - (MS09-004) Vulnerability In Microsoft SQL Server Could Allow Remote Code Execution (959420)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-5416

Update Details

Recommendation is updated

7374 - (MS09-018) Vulnerabilities In Active Directory Could Allow Remote Code Execution (971055)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1138, CVE-2009-1139

Update Details

Recommendation is updated

7377 - (MS09-019) Cumulative Security Update for Internet Explorer (969897)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3091, CVE-2009-1140, CVE-2009-1141, CVE-2009-1528, CVE-2009-1529, CVE-2009-1530, CVE-2009-1531, CVE-2009-1532

Update Details

Recommendation is updated

7383 - (MS09-021) Vulnerabilities In Microsoft Office Excel Could Allow Remote Code Execution (969462)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0549, CVE-2009-0557, CVE-2009-0558, CVE-2009-0559, CVE-2009-0560, CVE-2009-0561, CVE-2009-1134

Update Details

Recommendation is updated

7384 - (MS09-022) Vulnerabilities In Windows Print Spooler Could Allow Remote Code Execution (961501)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0228, CVE-2009-0229, CVE-2009-0230

Update Details

Recommendation is updated

7412 - (MS09-005) Vulnerabilities In Microsoft Office Visio Could Allow Remote Code Execution (957634)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0095, CVE-2009-0096, CVE-2009-0097

Update Details

Recommendation is updated

7413 - (MS09-006) Vulnerabilities In Windows Kernel Could Allow Remote Code Execution (958690)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0081, CVE-2009-0082, CVE-2009-0083

Update Details

Recommendation is updated

7416 - (MS09-009) Vulnerabilities In Microsoft Office Excel Could Cause Remote Code Execution (968557)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0100, CVE-2009-0238

Update Details

Recommendation is updated

7417 - (MS09-010) Vulnerabilities In WordPad And Office Text Converters Could Allow Remote Code Execution (960477)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4841, CVE-2009-0087, CVE-2009-0088, CVE-2009-0235

Update Details

Recommendation is updated

7418 - (MS09-011) Vulnerability In Microsoft DirectShow Could Allow Remote Code Execution (961373)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0084

Update Details

Recommendation is updated

7423 - (MS09-039) Vulnerabilities In WINS Could Allow Remote Code Execution (969883)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1923, CVE-2009-1924

Update Details

Recommendation is updated

7425 - (MS09-041) Vulnerability In Workstation Service Could Allow Elevation Of Privilege (971657)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1544

Update Details

Recommendation is updated

7427 - (MS09-044) Vulnerabilities In Remote Desktop Connection Could Allow Remote Code Execution (970927)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1133, CVE-2009-1929

Update Details

Recommendation is updated

7449 - (MS09-074) Project Memory Validation Vulnerability (967183)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0102

Update Details

Recommendation is updated

7451 - (MS09-070) Remote Code Execution in ADFS Vulnerability (971726)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2509

Update Details

Recommendation is updated

7455 - (MS09-073) WordPad and Office Text converter Memory Corruption Vulnerability (975539)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2506

Update Details

Recommendation is updated

7456 - (MS09-072) ATL COM Initialization Vulnerability (976325)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2493

Update Details

Recommendation is updated

7457 - (MS09-072) Uninitialized Memory Corruption Vulnerability (976325)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3671

Update Details

Recommendation is updated

7458 - (MS09-072) HTML Object Memory Corruption Vulnerability (976325)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3672

Update Details

Recommendation is updated

7459 - (MS09-072) Uninitialized Memory Corruption Vulnerability III (976325)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3673

Update Details

Recommendation is updated

7460 - (MS09-072) Uninitialized Memory Corruption Vulnerability II (976325)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3674

Update Details

Recommendation is updated

7461 - (MS09-074) Vulnerability In Microsoft Office Project Could Allow Remote Code Execution (967183)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0102

Update Details

Recommendation is updated

7462 - (MS09-070) Vulnerabilities In Active Directory Federation Services Could Allow Remote Code Execution (971726)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2508, CVE-2009-2509

Update Details

Recommendation is updated

7465 - (MS09-073) Vulnerability In WordPad And Office Text Converters Could Allow Remote Code Execution (975539)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2506

Update Details

Recommendation is updated

7466 - (MS09-072) Cumulative Security Update For Internet Explorer (976325)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2493, CVE-2009-3671, CVE-2009-3672, CVE-2009-3673, CVE-2009-3674

Update Details

Recommendation is updated

7529 - (MS09-035) Vulnerabilities In Visual Studio Active Template Library Could Allow Remote Code Execution (969706)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0901, CVE-2009-2493, CVE-2009-2495

Update Details

Recommendation is updated

7531 - (MS09-043) Vulnerabilities In Microsoft Office Web Components Could Allow Remote Code Execution (957638)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1136, CVE-2009-0562, CVE-2009-1534, CVE-2009-2496

Update Details

Recommendation is updated

7543 - (MS09-024) Vulnerability In Microsoft Works Converters Could Allow Remote Code Execution (957632)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1533

Update Details

Recommendation is updated

7547 - (MS09-028) Vulnerabilities In Microsoft DirectShow Could Allow Remote Code Execution (971633)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1537, CVE-2009-1538, CVE-2009-1539

Update Details

Recommendation is updated

7548 - (MS09-029) Vulnerabilities In The Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0231, CVE-2009-0232

Update Details

Recommendation is updated

7549 - (MS09-030) Vulnerability In Microsoft Office Publisher Could Allow Remote Code Execution (969516)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0566

Update Details

Recommendation is updated

7550 - (MS09-031) Vulnerability In Microsoft ISA Server 2006 Could Cause Elevation Of Privilege (970953)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1135

Update Details

Recommendation is updated

7552 - (MS09-033) Vulnerability In Virtual PC And Virtual Server Could Allow Elevation Of Privilege (969856)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1542

Update Details

Recommendation is updated

7623 - (MS08-001) Vulnerabilities In Windows TCP/IP Could Allow Remote Code Execution (941644)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0066, CVE-2007-0069

Update Details

Recommendation is updated

7635 - (MS08-049) Vulnerabilities In Event System Could Allow Remote Code Execution (950974)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1457, CVE-2008-1456

Update Details

Recommendation is updated

7639 - (MS08-051) Vulnerabilities In Microsoft PowerPoint Could Allow Remote Code Execution (949785)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0120, CVE-2008-0121, CVE-2008-1455

Update Details

Recommendation is updated

7642 - (MS10-001) Vulnerability In the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0018

Update Details

Recommendation is updated

7643 - (MS10-001) Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0018

Update Details

Recommendation is updated

7644 - (MS08-020) Vulnerability In DNS Client Could Allow Spoofing (945553)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0087

Update Details

Recommendation is updated

7647 - (MS08-022) Vulnerability In VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0083

Update Details

Recommendation is updated

7701 - (MS08-052) Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

7706 - (MS08-053) Vulnerability In Windows Media Encoder 9 Could Allow Remote Code Execution (954156)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3008

Update Details

Recommendation is updated

7707 - (MS08-054) Vulnerability In Windows Media Player Could Allow Remote Code Execution (954154)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2253

Update Details

Recommendation is updated

7772 - (MS08-027) Vulnerability In Microsoft Publisher Could Allow Remote Code Execution (951208)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0119

Update Details

Recommendation is updated

7773 - (MS08-028) Vulnerability In Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-6026

Update Details

Recommendation is updated

7804 - (MS08-031) Cumulative Security Update For Internet Explorer (950759)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1442, CVE-2008-1544

Update Details

Recommendation is updated

7808 - (MS08-033) Vulnerabilities In DirectX Could Allow Remote Code Execution (951698)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0011, CVE-2008-1444

Update Details

Recommendation is updated

7809 - (MS08-055) Vulnerability in Microsoft Office Could Allow Remote Code Execution (955047)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3007

Update Details

Recommendation is updated

7822 - (MS08-009) Vulnerability In Microsoft Word Could Allow Remote Code Execution (947077)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0109

Update Details

Recommendation is updated

7825 - (MS08-010) Cumulative Security Update For Internet Explorer (944533)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-4790, CVE-2008-0076, CVE-2008-0077, CVE-2008-0078

Update Details

Recommendation is updated

7827 - (MS08-018) Vulnerability In Microsoft Project Could Allow Remote Code Execution (950183)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1088

Update Details

Recommendation is updated

7829 - (MS08-011) Vulnerabilities In Microsoft Works File Converter Could Allow Remote Code Execution (947081)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0216, CVE-2008-0105, CVE-2008-0108

Update Details

Recommendation is updated

7830 - (MS08-037) Vulnerabilities In DNS Could Allow Spoofing (953230)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1447, CVE-2008-1454

Update Details

Recommendation is updated

7831 - (MS08-038) Vulnerability In Windows Explorer Could Allow Remote Code Execution (950582)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1435

Update Details

Recommendation is updated

7832 - (MS08-012) Vulnerabilities In Microsoft Office Publisher Could Allow Remote Code Execution (947085)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0102, CVE-2008-0104

Update Details

Recommendation is updated

7833 - (MS08-013) Vulnerability In Microsoft Office Could Allow Remote Code Execution (947108)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0103

Update Details

Recommendation is updated

7834 - (MS08-015) Vulnerability In Microsoft Outlook Could Allow Remote Code Execution (949031)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0110

Update Details

Recommendation is updated

7851 - (MS10-007) Microsoft Windows URL Validation Vulnerability (975713)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0027

Update Details

Recommendation is updated

7854 - (MS10-013) Microsoft Windows DirectShow Heap Overflow Vulnerability (977935)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0250

Update Details

Recommendation is updated

7856 - (MS10-003) Microsoft Office MSO.DLL Buffer Overflow (978214)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0243

Update Details

Recommendation is updated

7857 - (MS10-006) Microsoft Windows SMB Client Pool Corruption Vulnerability (978251)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0016

Update Details

Recommendation is updated

7858 - (MS10-006) Microsoft Windows SMB Client Race Condition Vulnerability (978251)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0017

Update Details

Recommendation is updated

7859 - (MS10-005) Microsoft Office Paint Integer Overflow Vulnerability (978706)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0028

Update Details

Recommendation is updated

7862 - (MS10-034) Microsoft Windows Data Analyzer ActiveX Control Vulnerability (980195)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0252

Update Details

Recommendation is updated

7872 - (MS10-004) Microsoft Office PowerPoint LinkedSlideAtom Heap Overflow Vulnerability (975416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0030

Update Details

Recommendation is updated

7873 - (MS10-004) Microsoft Office PowerPoint OEPlaceholderAtom 'placementId' Invalid Array Indexing Vulnerability (975416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0031

Update Details

Recommendation is updated

7874 - (MS10-004) Microsoft Office PowerPoint OEPlaceholderAtom Use After Free Vulnerability (975416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0032

Update Details

Recommendation is updated

7875 - (MS10-004) Microsoft Office PowerPoint Viewer TextBytesAtom Record Stack Overflow Vulnerability (975416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0033

Update Details

Recommendation is updated

7876 - (MS10-004) Microsoft Office PowerPoint Viewer TextCharsAtom Record Stack Overflow Vulnerability (975416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0034

Update Details

Recommendation is updated

7877 - (MS10-003) Vulnerability In Microsoft Office (MSO) Could Allow Remote Code Execution (978214)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0243

Update Details

Recommendation is updated

7878 - (MS10-004) Vulnerabilities In Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0029, CVE-2010-0030, CVE-2010-0031, CVE-2010-0032, CVE-2010-0033, CVE-2010-0034

Update Details

Recommendation is updated

7879 - (MS10-005) Vulnerability In Microsoft Paint Could Allow Remote Code Execution (978706)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0028

Update Details

Recommendation is updated

7880 - (MS10-006) Vulnerabilities In SMB Client Could Allow Remote Code Execution (978251)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0016, CVE-2010-0017

Update Details

Recommendation is updated

7881 - (MS10-007) Vulnerability In Windows Shell Handler Could Allow Remote Code Execution (975713)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0027

Update Details

Recommendation is updated

7886 - (MS10-012) Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231

Update Details

Recommendation is updated

7887 - (MS10-013) Vulnerability In Microsoft DirectShow Could Allow Remote Code Execution (977935)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0250

Update Details

Recommendation is updated

7940 - (MS08-016) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (949030)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0113, CVE-2008-0118

Update Details

Recommendation is updated

7942 - (MS08-017) Vulnerabilities In Microsoft Office Web Components Could Allow Remote Code Execution (933103)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4695, CVE-2007-1201

Update Details

Recommendation is updated

7943 - (MS08-040) Vulnerabilities In Microsoft SQL Server Could Allow Elevation Of Privilege (941203)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0085, CVE-2008-0086, CVE-2008-0106, CVE-2008-0107

Update Details

Recommendation is updated

8017 - (MS08-042) Vulnerability In Microsoft Word Could Allow Remote Code Execution (955048)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2244

Update Details

Recommendation is updated

8018 - (MS08-043) Vulnerabilities In Microsoft Excel Could Allow Remote Code Execution (954066)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3003, CVE-2008-3004, CVE-2008-3005, CVE-2008-3006

Update Details

Recommendation is updated

8020 - (MS08-058) Cumulative Security Update For Internet Explorer (956390)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2947, CVE-2008-3472, CVE-2008-3473, CVE-2008-3474, CVE-2008-3475, CVE-2008-3476

Update Details

Recommendation is updated

8051 - (MS08-062) Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution (953155)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1446

Update Details

Recommendation is updated

8098 - (MS08-044) Vulnerabilities In Microsoft Office Filters Could Allow Remote Code Execution (924090)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3018, CVE-2008-3019, CVE-2008-3020, CVE-2008-3021, CVE-2008-3460

Update Details

Recommendation is updated

8099 - (MS08-045) Cumulative Security Update For Internet Explorer (953838)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2254, CVE-2008-2255, CVE-2008-2256, CVE-2008-2257, CVE-2008-2258, CVE-2008-2259

Update Details

Recommendation is updated

8105 - (MS10-016) Microsoft Movie Maker Buffer Overflow Vulnerability (975561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0265

Update Details

Recommendation is updated

8106 - (MS10-017) Microsoft Office Excel Record Memory Corruption Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0257

Update Details

Recommendation is updated

8107 - (MS10-017) Microsoft Office Excel Sheet Object Type Confusion Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0258

Update Details

Recommendation is updated

8108 - (MS10-017) Microsoft Office Excel MDXTUPLE Record Heap Overflow Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0260

Update Details

Recommendation is updated

8109 - (MS10-017) Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0261

Update Details

Recommendation is updated

8110 - (MS10-017) Microsoft Office Excel FNGROUPNAME Record Uninitialized Memory Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0262

Update Details

Recommendation is updated

8111 - (MS10-017) Microsoft Office Excel XLSX File Parsing Code Execution Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0263

Update Details

Recommendation is updated

8112 - (MS10-017) Microsoft Office Excel DbOrParamQry Record Parsing Vulnerability (980150)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0264

Update Details

Recommendation is updated

8113 - (MS10-016) Vulnerability In Windows Movie Maker Could Allow Remote Code Execution (975561)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0265

Update Details

Recommendation is updated

8114 - (MS10-017) Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0257, CVE-2010-0258, CVE-2010-0260, CVE-2010-0261, CVE-2010-0262, CVE-2010-0263, CVE-2010-0264

Update Details

Recommendation is updated

8154 - (MS08-068) Vulnerability In SMB Could Allow Remote Code Execution (957097)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4037

Update Details

Recommendation is updated

8156 - (MS08-046) Vulnerability In Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2245

Update Details

Recommendation is updated

8168 - (MS08-069) Vulnerabilities In Microsoft XML Core Services Could Allow Remote Code Execution (955218)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0099, CVE-2008-4029, CVE-2008-4033

Update Details

Recommendation is updated

8180 - (MS08-070) Vulnerabilities In Visual Basic 6.0 Runtime Extended Files Could Allow Remote Code Execution (932349)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4252, CVE-2008-4253, CVE-2008-4254, CVE-2008-4255, CVE-2008-4256, CVE-2008-3704

Update Details

Recommendation is updated

8297 - (MS08-071) Vulnerabilities In GDI Could Allow Remote Code Execution (956802)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2249, CVE-2008-3465

Update Details

Recommendation is updated

8389 - (MS08-073) Cumulative Security Update For Internet Explorer (958215)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4258, CVE-2008-4259, CVE-2008-4260, CVE-2008-4261

Update Details

Recommendation is updated

8390 - (MS08-074) Vulnerabilities In Microsoft Office Excel Could Allow Remote Code Execution (959070)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4264, CVE-2008-4265, CVE-2008-4266

Update Details

Recommendation is updated

8391 - (MS08-075) Vulnerabilities In Windows Search Could Allow Remote Code Execution (959349)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4268, CVE-2008-4269

Update Details

Recommendation is updated

8516 - (MS10-026) Microsoft MPEG Layer-3 Audio Decoder Stack Overflow Vulnerability (977816)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0480

Update Details

Recommendation is updated

8533 - (MS10-025) Microsoft Windows Media Services Stack-based Buffer Overflow Vulnerability (980858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0478

Update Details

Recommendation is updated

8536 - (MS10-019) Microsoft Windows WinVerifyTrust Signature Validation Vulnerability (981210)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0486

Update Details

Recommendation is updated

8537 - (MS10-019) Microsoft Windows Cabview Corruption Validation Vulnerability (981210)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0487

Update Details

Recommendation is updated

8540 - (MS10-019) Vulnerabilities in Windows Could Allow Remote Code Execution (981210)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0486, CVE-2010-0487

Update Details

Recommendation is updated

8541 - (MS10-020) Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3676, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477

Update Details

Recommendation is updated

8542 - (MS10-025) Vulnerability in Microsoft Windows Media Services Could Allow Remote Code Execution (980858)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0478

Update Details

Recommendation is updated

8543 - (MS10-026) Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0480

Update Details

Recommendation is updated

8544 - (MS10-027) Vulnerability in Windows Media Player Could Allow Remote Code Execution (979402)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0268

Update Details

Recommendation is updated

8546 - (MS10-022) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0483

Update Details

Recommendation is updated

8549 - (MS10-028) Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (980094)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0254, CVE-2010-0256

Update Details

Recommendation is updated

8550 - (MS10-029) Vulnerabilities in Windows ISATAP Component Could Allow Spoofing (978338)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0256, CVE-2010-0812

Update Details

Recommendation is updated

8829 - (MS10-030) Vulnerability In Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0816

Update Details

Recommendation is updated

8831 - (MS10-030) Microsoft Outlook Express and Windows Mail Integer Overflow Vulnerability (978542)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0816

Update Details

Recommendation is updated

8913 - (MS10-043) Microsoft Windows Canonical Display Driver Code Execution Vulnerability (2028859)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3678

Update Details

Recommendation is updated

9065 - (MS10-035) Cumulative Security Update for Internet Explorer (982381)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0255, CVE-2010-1257, CVE-2010-1259, CVE-2010-1260, CVE-2010-1261, CVE-2010-1262

Update Details

Recommendation is updated

9066 - (MS10-036) Vulnerabilities In COM Validation In Microsoft Office Could Allow Remote Code Execution (983235)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1263

Update Details

Recommendation is updated

9068 - (MS10-034) Cumulative Security Update of ActiveX Kill Bits (980195)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0252, CVE-2010-0811

Update Details

Recommendation is updated

9071 - (MS10-038) Vulnerabilities In Microsoft Office Excel Could Allow Remote Code Execution (2027452)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0821, CVE-2010-0822, CVE-2010-0823, CVE-2010-0824, CVE-2010-1245, CVE-2010-1246

Update Details

Recommendation is updated

9072 - (MS10-033) Vulnerabilities In Media Decompression Could Allow Remote Code Execution (979902)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1879, CVE-2010-1880

Update Details

Recommendation is updated

9085 - (MS11-027) Microsoft Internet Explorer 8 Developer Tools Remote Code Execution (2508272)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0811

Update Details

Recommendation is updated

9087 - (MS10-040) Microsoft Windows IIS Authentication Memory Corruption Vulnerability (982666)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1256

Update Details

Recommendation is updated

9088 - (MS10-038) Microsoft Office Excel Record Parsing Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0821

Update Details

Recommendation is updated

9089 - (MS10-038) Microsoft Office Excel Object Stack Overflow Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0822

Update Details

Recommendation is updated

9090 - (MS10-038) Microsoft Office Excel Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0823

Update Details

Recommendation is updated

9091 - (MS10-038) Microsoft Office Excel Record Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0824

Update Details

Recommendation is updated

9092 - (MS10-038) Microsoft Office Excel Record Memory Corruption Vulnerability (2027452) CVE-2010-1245

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1245

Update Details

Recommendation is updated

9093 - (MS10-038) Microsoft Office Excel RTD Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1246

Update Details

Recommendation is updated

9094 - (MS10-038) Microsoft Excel Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1247

Update Details

Recommendation is updated

9095 - (MS10-038) Microsoft Excel HFPicture Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1248

Update Details

Recommendation is updated

9096 - (MS10-038) Microsoft Excel Memory Corruption Vulnerability II (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1249

Update Details

Recommendation is updated

9097 - (MS10-038) Microsoft Excel EDG Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1250

Update Details

Recommendation is updated

9098 - (MS10-038) Microsoft Excel Record Stack Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1251

Update Details

Recommendation is updated

9099 - (MS10-038) Microsoft Excel String Variable Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1252

Update Details

Recommendation is updated

9100 - (MS10-038) Microsoft Excel ADO Object Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1253

Update Details

Recommendation is updated

9102 - (MS10-033) Microsoft Windows Media Decompression Vulnerability (979902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1879

Update Details

Recommendation is updated

9103 - (MS10-033) Microsoft Windows MJPEG Media Decompression Vulnerability (979902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1880

Update Details

Recommendation is updated

9110 - (MS10-042) Microsoft Windows Help Center Escape Sequence Bypass Vulnerability (2219475)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1885

Update Details

Recommendation is updated

9415 - (MS10-042) Vulnerability In Help And Support Center Could Allow Remote Code Execution (2229593)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1885

Update Details

Recommendation is updated

9416 - (MS10-043) Vulnerability In Canonical Display Driver Could Allow Remote Code Execution (2032276)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3678

Update Details

Recommendation is updated

9417 - (MS10-044) Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1881, CVE-2010-0814

Update Details

Recommendation is updated

9418 - (MS10-045) Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0266

Update Details

Recommendation is updated

9419 - (MS10-044) Microsoft Office Access ActiveX Control Vulnerability (982335)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0814

Update Details

Recommendation is updated

9420 - (MS10-045) Microsoft Office Outlook SMB Attachment Vulnerability (978212)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0266

Update Details

Recommendation is updated

9421 - (MS10-044) Microsoft Office ACCWIZ.dll Uninitialized Variable Vulnerability (982335)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1881

Update Details

Recommendation is updated

9681 - (MS10-049) Microsoft Windows SChannel Malformed Certificate Request Remote Code Execution (980436)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2566

Update Details

Recommendation is updated

9685 - (MS10-050) Microsoft Windows Movie Maker Memory Corruption Remote Code Execution (981997)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2564

Update Details

Recommendation is updated

9689 - (MS10-055) Microsoft Windows Cinepak Codec Decompression Denial Of Service (982665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2553

Update Details

Recommendation is updated

9693 - (MS10-052) Microsoft Windows MPEG Layer-3 Audio Decoder Buffer Overflow Vulnerability (2115168)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1882

Update Details

Recommendation is updated

9699 - (MS10-053) Microsoft Internet Explorer HTML Layout Memory Corruption Vulnerability (2183461)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2560

Update Details

Recommendation is updated

9700 - (MS10-053) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (2183461)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2559

Update Details

Recommendation is updated

9701 - (MS10-053) Microsoft Internet Explorer Race Condition Memory Corruption Vulnerability (2183461)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2558

Update Details

Recommendation is updated

9702 - (MS10-053) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability CVE-2010-2557 (2183461)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2557

Update Details

Recommendation is updated

9703 - (MS10-053) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability CVE-2010-2556 (2183461)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2556

Update Details

Recommendation is updated

9705 - (MS10-060) Microsoft Windows Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability (22659

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1898

Update Details

Recommendation is updated

9706 - (MS10-060) Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (978464)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0019

Update Details

Recommendation is updated

9707 - (MS10-056) Microsoft Office Word HTML Linked Objects Memory Corruption Vulnerability (2269638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1903

Update Details

Recommendation is updated

9708 - (MS10-056) Microsoft Office Word RTF Parsing Buffer Overflow Vulnerability (2269638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1902

Update Details

Recommendation is updated

9709 - (MS10-056) Microsoft Office Word RTF Parsing Engine Memory Corruption Vulnerability (2269638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1901

Update Details

Recommendation is updated

9710 - (MS10-056) Microsoft Office Word Record Parsing Vulnerability (2269638)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1900

Update Details

Recommendation is updated

9711 - (MS10-057) Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (2269707)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2562

Update Details

Recommendation is updated

9713 - (MS10-049) Vulnerabilities in SChannel could allow Remote Code Execution (980436)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3555, CVE-2010-2566

Update Details

Recommendation is updated

9716 - (MS10-050) Vulnerability in Movie Maker Could Allow Remote Code Execution (981997)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2564

Update Details

Recommendation is updated

9717 - (MS10-054) Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2550, CVE-2010-2551, CVE-2010-2552

Update Details

Recommendation is updated

9718 - (MS10-055) Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2553

Update Details

Recommendation is updated

9720 - (MS10-051) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2561

Update Details

Recommendation is updated

9721 - (MS10-052) Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1882

Update Details

Recommendation is updated

9723 - (MS10-053) Cumulative Security Update for Internet Explorer (2183461)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1258, CVE-2010-2556, CVE-2010-2557, CVE-2010-2558, CVE-2010-2559, CVE-2010-2560

Update Details

Recommendation is updated

9724 - (MS10-060) Vulnerabilities In Microsoft Silverlight And .NET CLR Could Allow Remote Code Execution (2265906)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0019, CVE-2010-1898

Update Details

Recommendation is updated

9725 - (MS10-056) Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1900, CVE-2010-1901, CVE-2010-1902, CVE-2010-1903

Update Details

Recommendation is updated

10041 - (MS10-063) Microsoft Windows Uniscribe Font Parsing Engine Memory Corruption Remote Code Execution (2320113)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2738

Update Details

Recommendation is updated

10042 - (MS10-062) Microsoft Windows MPEG-4 Codec Remote Code Execution (975558)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0818

Update Details

Recommendation is updated

10043 - (MS10-068) Microsoft Windows LSASS Heap Overflow Privilege Escalation (983539)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0820

Update Details

Recommendation is updated

10044 - (MS10-067) Microsoft Windows WordPad Word 97 Text Converter Memory Corruption Remote Code Execution (2259922)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2563

Update Details

Recommendation is updated

10045 - (MS10-064) Microsoft Office Heap Based Buffer Overflow in Outlook Remote Code Execution (2315011)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2728

Update Details

Recommendation is updated

10046 - (MS10-061) Microsoft Windows Print Spooler Service Impersonation Remote Code Execution (2347290)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2729

Update Details

Recommendation is updated

10047 - (MS10-066) Microsoft Windows RPC Memory Corruption Remote Code Execution (982802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2567

Update Details

Recommendation is updated

10049 - (MS10-065) Vulnerabilities In Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1899, CVE-2010-2730, CVE-2010-2731

Update Details

Recommendation is updated

10050 - (MS10-063) Vulnerability In Unicode Scripts Processor Could Lead To Remote Code Execution (2320113)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2738

Update Details

Recommendation is updated

10051 - (MS10-062) Vulnerability In MPEG-4 Codec Could Allow Remote Code Execution (975558)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0818

Update Details

Recommendation is updated

10052 - (MS10-068) Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0820

Update Details

Recommendation is updated

10053 - (MS10-067) Vulnerability In WordPad Text Converters Could Allow Remote Code Execution (2259922)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2563

Update Details

Recommendation is updated

10054 - (MS10-064) Vulnerability In Microsoft Outlook Could Allow Remote Code Execution (2315011)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2728

Update Details

Recommendation is updated

10055 - (MS10-061) Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2729

Update Details

Recommendation is updated

10056 - (MS10-066) Vulnerability In Remote Procedure Call Could Allow Remote Code Execution (982802)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2567

Update Details

Recommendation is updated

10315 - (MS10-074) Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3227

Update Details

Recommendation is updated

10316 - (MS10-074) Microsoft Windows MFC Document Title Updating Buffer Overflow Vulnerability (2387149)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3227

Update Details

Recommendation is updated

10319 - (MS10-077) Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3228

Update Details

Recommendation is updated

10322 - (MS10-071) Cumulative Security Update for Internet Explorer (2360131)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0808, CVE-2010-3243, CVE-2010-3324, CVE-2010-3325, CVE-2010-3326, CVE-2010-3327, CVE-2010-3328, CVE-2010-3329, CVE-2010-3330, CVE-2010-3331

Update Details

Recommendation is updated

10323 - (MS10-083) Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1263

Update Details

Recommendation is updated

10324 - (MS10-083) Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (2405882)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1263

Update Details

Recommendation is updated

10325 - (MS10-082) Microsoft Windows Media Player Memory Corruption Remote Code Execution (2378111)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2745

Update Details

Recommendation is updated

10326 - (MS10-082) Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2745

Update Details

Recommendation is updated

10331 - (MS10-079) Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2747, CVE-2010-2748, CVE-2010-2750, CVE-2010-3214, CVE-2010-3215, CVE-2010-3216, CVE-2010-3217, CVE-2010-3218 , CVE-2010-3219 , CVE-2010-3220 , CVE-2010-3221

Update Details

Recommendation is updated

10332 - (MS10-079) Microsoft Office Word Uninitialized Pointer Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2747

Update Details

Recommendation is updated

10333 - (MS10-079) Microsoft Office Word Boundary Check Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2748

Update Details

Recommendation is updated

10334 - (MS10-079) Microsoft Office Word Index Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2750

Update Details

Recommendation is updated

10335 - (MS10-079) Microsoft Office Word Stack Validation Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3214

Update Details

Recommendation is updated

10336 - (MS10-079) Microsoft Office Word Return Value Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3215

Update Details

Recommendation is updated

10337 - (MS10-079) Microsoft Office Word Bookmarks Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3216

Update Details

Recommendation is updated

10338 - (MS10-079) Microsoft Office Word Pointer Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3217

Update Details

Recommendation is updated

10339 - (MS10-079) Microsoft Office Word Heap Overflow Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3218

Update Details

Recommendation is updated

10340 - (MS10-079) Microsoft Office Word Index Parsing Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3219

Update Details

Recommendation is updated

10341 - (MS10-079) Microsoft Office Word Parsing Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3220

Update Details

Recommendation is updated

10342 - (MS10-079) Microsoft Office Word Short Sign Remote Code Execution (2293194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3221

Update Details

Recommendation is updated

10344 - (MS10-077) Microsoft .NET Framework x64 JIT Compiler Remote Code Execution (2160841)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3228

Update Details

Recommendation is updated

10349 - (MS10-071) Microsoft Internet Explorer Uninitialized Memory Corruption Remote Code Execution (2360131) I

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3326

Update Details

Recommendation is updated

10350 - (MS10-071) Microsoft Internet Explorer Uninitialized Memory Corruption Remote Code Execution (2360131) II

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3328

Update Details

Recommendation is updated

10352 - (MS10-071) Microsoft Internet Explorer Uninitialized Memory Corruption Remote Code Execution (2360131) III

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3329

Update Details

Recommendation is updated

10354 - (MS10-071) Microsoft Internet Explorer Uninitialized Memory Corruption (2360131) IV

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3331

Update Details

Recommendation is updated

10355 - (MS10-076) Microsoft Embedded OpenType Font Integer Overflow Remote Code Execution (982132)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1883

Update Details

Recommendation is updated

10356 - (MS10-076) Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1883

Update Details

Recommendation is updated

10357 - (MS10-080) Microsoft Office Excel Record Parsing Integer Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3230

Update Details

Recommendation is updated

10359 - (MS10-080) Microsoft Office Excel Record Parsing Memory Corruption (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3231

Update Details

Recommendation is updated

10367 - (MS10-080) Microsoft Office Excel File Format Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3232

Update Details

Recommendation is updated

10368 - (MS10-080) Microsoft Office Lotus 1-2-3 Workbook Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3233

Update Details

Recommendation is updated

10369 - (MS10-080) Microsoft Office Formula Substream Memory Corruption (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3234

Update Details

Recommendation is updated

10370 - (MS10-080) Microsoft Office Formula Biff Record Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3235

Update Details

Recommendation is updated

10373 - (MS10-080) Microsoft Office Out Of Bounds Array Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3236

Update Details

Recommendation is updated

10374 - (MS10-080) Microsoft Office Merge Cell Record Pointer Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3237

Update Details

Recommendation is updated

10375 - (MS10-080) Microsoft Office Negative Future Function Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3238

Update Details

Recommendation is updated

10379 - (MS10-080) Microsoft Office Extra Out of Boundary Record Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3239

Update Details

Recommendation is updated

10380 - (MS10-080) Microsoft Office Real Time Data Array Record Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3240

Update Details

Recommendation is updated

10381 - (MS10-080) Microsoft Office Out-of-Bounds Memory Write in Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3241

Update Details

Recommendation is updated

10382 - (MS10-080) Microsoft Office Ghost Record Type Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3242

Update Details

Recommendation is updated

10383 - (MS10-080) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3230, CVE-2010-3231, CVE-2010-3232, CVE-2010-3233, CVE-2010-3234, CVE-2010-3235, CVE-2010-3236, CVE-2010-3237, CVE-2010-3238, CVE-2010-3239, CVE-2010-3240, CVE-2010-3241, CVE-2010-3242

Update Details

Recommendation is updated

10385 - (MS10-061) Microsoft Windows Print Spooler Service Impersonation (2347290)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2010-2729

Update Details

Recommendation is updated

10618 - (MS10-090) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3962

Update Details

Recommendation is updated

10653 - (MS10-087) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2423930)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3333, CVE-2010-3334, CVE-2010-3335, CVE-2010-3336, CVE-2010-3337

Update Details

Recommendation is updated

10654 - (MS10-088) Vulnerabilities In Microsoft PowerPoint Could Allow Remote Code Execution (2293386)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2572, CVE-2010-2573

Update Details

Recommendation is updated

10855 - (MS10-090) Cumulative Security Update For Internet Explorer (2416400)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3340, CVE-2010-3342, CVE-2010-3343, CVE-2010-3345, CVE-2010-3346, CVE-2010-3348, CVE-2010-3962

Update Details

Recommendation is updated

10856 - (MS10-091) Vulnerabilities In The OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3956, CVE-2010-3957, CVE-2010-3959

Update Details

Recommendation is updated

10858 - (MS10-093) Vulnerability In Windows Movie Maker Could Allow Remote Code Execution (2424434)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3967

Update Details

Recommendation is updated

10859 - (MS10-094) Vulnerability In Windows Media Encoder Could Allow Remote Code Execution (2447961)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3965

Update Details

Recommendation is updated

10862 - (MS10-095) Vulnerability In Microsoft Windows Could Allow Remote Code Execution (2385678)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3966

Update Details

Recommendation is updated

10863 - (MS10-105) Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3945, CVE-2010-3946 , CVE-2010-3947, CVE-2010-3949, CVE-2010-3950, CVE-2010-3951, CVE-2010-3952

Update Details

Recommendation is updated

10864 - (MS10-104) Vulnerability in Microsoft SharePoint Could Allow Remote Code Execution (2455005)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3964

Update Details

Recommendation is updated

10865 - (MS10-103) Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2569, CVE-2010-2570, CVE-2010-2571 , CVE-2010-3954, CVE-2010-3955

Update Details

Recommendation is updated

10866 - (MS10-096) Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3147

Update Details

Recommendation is updated

10868 - (MS10-097) Insecure Library Loading In Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3144

Update Details

Recommendation is updated

10871 - (MS10-105) Microsoft Office Graphics Filters CGM Image Converter Buffer Overrun Vulnerability (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3945

Update Details

Recommendation is updated

10872 - (MS10-105) Microsoft Office Graphics PICT Image Converter Integer Overflow Vulnerability (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3946

Update Details

Recommendation is updated

10873 - (MS10-105) Microsoft Office Graphics TIFF Image Converter Heap Overflow Vulnerability (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3947

Update Details

Recommendation is updated

10874 - (MS10-105) Microsoft Office Graphics TIFF Image Converter Buffer Overflow Vulnerability (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3949

Update Details

Recommendation is updated

10875 - (MS10-105) Microsoft Office Graphics TIFF Image Converter Memory Corruption Vulnerability (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3950

Update Details

Recommendation is updated

10876 - (MS10-105) Microsoft Office Graphics FlashPix Image Converter Buffer Overflow Vulnerability (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3951

Update Details

Recommendation is updated

10877 - (MS10-105) Microsoft Office Graphics FlashPix Image Converter Heap Corruption Vulnerability I (968095)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3952

Update Details

Recommendation is updated

10879 - (MS10-103) Microsoft Office Suites and Components Size Value Heap Corruption in pubconv.dll Vulnerability (2292970)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2569

Update Details

Recommendation is updated

10880 - (MS10-103) Microsoft Office Suites Heap Overrun in pubconv.dll Vulnerability (2292970)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2570

Update Details

Recommendation is updated

10881 - (MS10-103) Microsoft Office Suites Memory Corruption Due To Invalid Index Into Array in Pubconv.dll Vulnerability (2292970)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2571

Update Details

Recommendation is updated

10882 - (MS10-103) Microsoft Publisher Memory Corruption Vulnerability (2292970)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3954

Update Details

Recommendation is updated

10883 - (MS10-103) Microsoft Office Suites Array Indexing Memory Corruption Vulnerability (2292970)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3955

Update Details

Recommendation is updated

10884 - (MS10-091) Microsoft Windows OpenType Font Index Vulnerability (2296199)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3956

Update Details

Recommendation is updated

10888 - (MS10-095) Microsoft Windows BranchCache Insecure Library Loading Could Allow Remote Code Execution (2385678)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3966

Update Details

Recommendation is updated

10890 - (MS10-090) Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability CVE-2010-3340 (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3340

Update Details

Recommendation is updated

10892 - (MS10-090) Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability CVE-2010-3343 (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3343

Update Details

Recommendation is updated

10893 - (MS10-090) Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability CVE-2010-3345 (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3345

Update Details

Recommendation is updated

10894 - (MS10-090) Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability CVE-2010-3346 (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3346

Update Details

Recommendation is updated

10896 - (MS10-096) Microsoft Windows Address Book Could Allow Remote Code Execution (2423089)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3147

Update Details

Recommendation is updated

10897 - (MS10-093) Microsoft Windows Movie Maker Could Allow Remote Code Execution (2424434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3967

Update Details

Recommendation is updated

10904 - (MS10-100) Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3961

Update Details

Recommendation is updated

10907 - (MS10-097) Microsoft Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3144

Update Details

Recommendation is updated

10908 - (MS10-094) Microsoft Windows Media Encoder Could Allow Remote Code Execution (2447961)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3965

Update Details

Recommendation is updated

10916 - (MS11-002) Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0026, CVE-2011-0027

Update Details

Recommendation is updated

10938 - (MS11-003) Microsoft Internet Explorer CSS Memory Corruption (2482017)

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3971

Update Details

Recommendation is updated

10998 - (MS11-001) Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3145

Update Details

Recommendation is updated

10999 - (MS11-002) Microsoft Data Access DSN Buffer Overflow (2451910)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0026

Update Details

Recommendation is updated

11000 - (MS11-002) Microsoft Data Access ADO Record Memory Allocation (2451910)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0027

Update Details

Recommendation is updated

11001 - (MS11-001) Windows Backup Manager Insecure Library Loading (2478935)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3145

Update Details

Recommendation is updated

11066 - (MS10-036) Microsoft Office COM Object Validation Vulnerability (983235)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1263

Update Details

Recommendation is updated

11238 - (MS11-008) Microsoft Visio Object Memory Corruption (2451879)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0092

Update Details

Recommendation is updated

11239 - (MS11-008) Microsoft Visio Data Type Memory Corruption (2451879)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0093

Update Details

Recommendation is updated

11249 - (MS11-003) Microsoft Internet Explorer Uninitialized Memory Corruption I (2482017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0035

Update Details

Recommendation is updated

11250 - (MS11-003) Microsoft Internet Explorer Uninitialized Memory Corruption II (2482017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0036

Update Details

Recommendation is updated

11251 - (MS11-003) Microsoft Internet Explorer Insecure Library Loading (2482017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0038

Update Details

Recommendation is updated

11252 - (MS11-007) Microsoft OpenType Font Encoded Character (2485376)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0033

Update Details

Recommendation is updated

11254 - (MS11-008) Vulnerabilities In Microsoft Visio Could Allow Remote Code Execution (2451879)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0092, CVE-2011-0093

Update Details

Recommendation is updated

11267 - (MS11-003) Cumulative Security Update For Internet Explorer (2482017)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3971, CVE-2011-0035, CVE-2011-0036, CVE-2011-0038

Update Details

Recommendation is updated

11268 - (MS11-007) Vulnerability In The OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0033

Update Details

Recommendation is updated

11269 - (MS11-004) Vulnerability In Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3972

Update Details

Recommendation is updated

11271 - (MS11-006) Vulnerability In Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3970

Update Details

Recommendation is updated

11340 - (MS11-022) Microsoft PowerPoint OfficeArt Atom RCE (2489283)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0976

Update Details

Recommendation is updated

11341 - (MS11-023) Microsoft Office Graphic Object Dereferencing (2489293)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0977

Update Details

Recommendation is updated

11342 - (MS11-021) Microsoft Excel Array Indexing (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0978

Update Details

Recommendation is updated

11343 - (MS11-021) Microsoft Excel Linked List Corruption (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0979

Update Details

Recommendation is updated

11344 - (MS11-021) Microsoft Excel Dangling Pointer (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0980

Update Details

Recommendation is updated

11527 - (MS11-015) Vulnerabilities In Windows Media Could Allow Remote Code Execution (2510030)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0032

Update Details

Recommendation is updated

11528 - (MS11-016) Vulnerability In Microsoft Office Groove Could Allow Remote Code Execution (2494047)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0108

Update Details

Recommendation is updated

11529 - (MS11-017) Vulnerability In Remote Desktop Client Could Allow Remote Code Execution (2508062)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0029

Update Details

Recommendation is updated

11530 - (MS11-016) Microsoft Microsoft Groove Insecure Library Loading RCE (2494047)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3146

Update Details

Recommendation is updated

11531 - (MS11-017) Microsoft Remote Desktop Client Insecure Library Loading (2508062)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0029

Update Details

Recommendation is updated

11532 - (MS11-015) Microsoft Windows Media DVR-MS (2510030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0042

Update Details

Recommendation is updated

11533 - (MS11-015) Microsoft Windows Media DirectShow Insecure Library Loading (2510030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0032

Update Details

Recommendation is updated

11580 - (MS11-018) Microsoft Internet Explorer Object Management Memory Corruption (2497640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1345

Update Details

Recommendation is updated

11754 - (MS11-018) Cumulative Security Update For Internet Explorer (2497640)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0094, CVE-2011-0346, CVE-2011-1244, CVE-2011-1245, CVE-2011-1345

Update Details

Recommendation is updated

11756 - (MS11-020) Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0661

Update Details

Recommendation is updated

11757 - (MS11-021) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0097, CVE-2011-0098, CVE-2011-0101, CVE-2011-0103, CVE-2011-0104, CVE-2011-0105, CVE-2011-0978, CVE-2011-0979, CVE-2011-0980

Update Details

Recommendation is updated

11758 - (MS11-022) Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2489283)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0655, CVE-2011-0656, CVE-2011-0976

Update Details

Recommendation is updated

11759 - (MS11-023) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2489293)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0107, CVE-2011-0977

Update Details

Recommendation is updated

11760 - (MS11-024) Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3974, CVE-2010-4701

Update Details

Recommendation is updated

11761 - (MS11-025) Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3190

Update Details

Recommendation is updated

11763 - (MS11-027) Cumulative Security Update of ActiveX Kill Bits (2508272)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0811, CVE-2010-3973, CVE-2011-1243

Update Details

Recommendation is updated

11764 - (MS11-028) Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3958

Update Details

Recommendation is updated

11765 - (MS11-029) Vulnerability in GDI+ Could Allow Remote Code Execution (2489979)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0041

Update Details

Recommendation is updated

11766 - (MS11-030) Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0657

Update Details

Recommendation is updated

11767 - (MS11-031) Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0663

Update Details

Recommendation is updated

11768 - (MS11-032) Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0034

Update Details

Recommendation is updated

11773 - (MS11-028) Microsoft .NET Framework Stack Corruption (2484015)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3958

Update Details

Recommendation is updated

11774 - (MS11-033) Microsoft WordPad Converter Parsing (2485663)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0028

Update Details

Recommendation is updated

11775 - (MS11-021) Microsoft Excel Integer Overrun (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0097

Update Details

Recommendation is updated

11777 - (MS11-021) Microsoft Excel Record Parsing WriteAV (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0101

Update Details

Recommendation is updated

11778 - (MS11-021) Microsoft Excel Memory Corruption (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0103

Update Details

Recommendation is updated

11779 - (MS11-021) Microsoft Excel Heap Overflow (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0098

Update Details

Recommendation is updated

11780 - (MS11-021) Microsoft Excel Buffer Overwrite (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0104

Update Details

Recommendation is updated

11781 - (MS11-021) Microsoft Excel Data Initialization (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0105

Update Details

Recommendation is updated

11782 - (MS11-022) Microsoft PowerPoint Floating Point Techno-color Time Bandit RCE (2489283)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0655

Update Details

Recommendation is updated

11783 - (MS11-022) Microsoft PowerPoint Persist Directory RCE (2489283)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0656

Update Details

Recommendation is updated

11784 - (MS11-023) Microsoft Office Component Insecure Library Loading (2489293)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0107

Update Details

Recommendation is updated

11785 - (MS11-029) Microsoft GDI+ Integer Overflow (2489979)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0041

Update Details

Recommendation is updated

11787 - (MS11-018) Microsoft Internet Explorer Layouts Handling Memory Corruption (2497640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0094

Update Details

Recommendation is updated

11788 - (MS11-018) Microsoft Internet Explorer MSHTML Memory Corruption (2497640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0346

Update Details

Recommendation is updated

11790 - (MS11-025) Microsoft MFC Insecure Library Loading (2500212)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3190

Update Details

Recommendation is updated

11820 - (MS11-032) Microsoft OpenType Font Stack Overflow Remote Code Execution (2507618)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0034

Update Details

Recommendation is updated

11821 - (MS11-027) Microsoft WMITools ActiveX Control Remote Code Execution (2508272)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3973

Update Details

Recommendation is updated

11822 - (MS11-027) Microsoft Windows Messenger ActiveX Control Remote Code Execution (2508272)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1243

Update Details

Recommendation is updated

11826 - (MS11-019) Microsoft SMB Client Response Parsing Remote Code Execution (2511455)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0660

Update Details

Recommendation is updated

11827 - (MS11-031) Microsoft Scripting Engines Memory Reallocation Remote Code Execution (2514666)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0663

Update Details

Recommendation is updated

11992 - (MS11-035) Microsoft WINS Service Failed Response (2524426)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1248

Update Details

Recommendation is updated

11993 - (MS11-036) Microsoft PowerPoint Buffer Overrun RCE (2545814)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1270

Update Details

Recommendation is updated

11994 - (MS11-036) Microsoft PowerPoint Memory Corruption RCE (2545814)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1269

Update Details

Recommendation is updated

11996 - (MS11-036) Vulnerabilities In Microsoft PowerPoint Could Allow Remote Code Execution (2545814)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1269, CVE-2011-1270

Update Details

Recommendation is updated

12208 - (MS11-045) Microsoft Excel Buffer Overrun Remote Code Execution (2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1276

Update Details

Recommendation is updated

12209 - (MS11-045) Microsoft Excel Improper Record Parsing Remote Code Execution (KB2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1273

Update Details

Recommendation is updated

12210 - (MS11-045) Microsoft Excel Insufficient Record Validation Remote Code Execution (KB2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1272

Update Details

Recommendation is updated

12213 - (MS11-045) Microsoft Excel Memory Heap Overwrite Remote Code Execution (KB2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1275

Update Details

Recommendation is updated

12214 - (MS11-045) Microsoft Excel Out of Bounds Array Access Remote Code Execution (KB2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1274

Update Details

Recommendation is updated

12215 - (MS11-050) Cumulative Security Update for Internet Explorer (2530548)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1246, CVE-2011-1250, CVE-2011-1251, CVE-2011-1252, CVE-2011-1254, CVE-2011-1255, CVE-2011-1256, CVE-2011-1258, CVE-2011-1260, CVE-2011-1261, CVE-2011-1262

Update Details

Recommendation is updated

12216 - (MS11-038) Microsoft Windows OLE Automation Could Allow Remote Code Execution (2476490)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0658

Update Details

Recommendation is updated

12219 - (MS11-041) Microsoft Windows Kernel-Mode Drivers Could Allow Remote Code Execution (KB2525694)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1873

Update Details

Recommendation is updated

12226 - (MS11-038) Vulnerability In OLE Automation Could Allow Remote Code Execution (2476490)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0658

Update Details

Recommendation is updated

12227 - (MS11-052) Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1266

Update Details

Recommendation is updated

12228 - (MS11-039) Vulnerability In .NET Framework Could Allow Remote Code Execution (KB2514842)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0664

Update Details

Recommendation is updated

12233 - (MS11-050) Microsoft Internet Explorer Link Properties Handling Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1250

Update Details

Recommendation is updated

12234 - (MS11-050) Microsoft Internet Explorer DOM Manipulation Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1251

Update Details

Recommendation is updated

12236 - (MS11-050) Microsoft Internet Explorer Drag and Drop Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1254

Update Details

Recommendation is updated

12237 - (MS11-050) Microsoft Internet Explorer Time Element Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1255

Update Details

Recommendation is updated

12239 - (MS11-050) Microsoft Internet Explorer DOM Modification Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1256

Update Details

Recommendation is updated

12241 - (MS11-050) Microsoft Internet Explorer Layout Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1260

Update Details

Recommendation is updated

12242 - (MS11-050) Microsoft Internet Explorer Selection Object Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1261

Update Details

Recommendation is updated

12244 - (MS11-050) Microsoft Internet Explorer HTTP Redirect Memory Corruption (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1262

Update Details

Recommendation is updated

12246 - (MS11-052) Microsoft Internet Explorer VML Memory Corruption (2544521)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1266

Update Details

Recommendation is updated

12247 - (MS11-041) Vulnerability In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (KB2525694)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1873

Update Details

Recommendation is updated

12253 - (MS11-045) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2537146)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1272, CVE-2011-1273, CVE-2011-1274, CVE-2011-1275, CVE-2011-1276, CVE-2011-1277, CVE-2011-1278, CVE-2011-1279

Update Details

Recommendation is updated

12259 - (MS11-039) Microsoft Windows .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0664

Update Details

Recommendation is updated

12340 - (MS11-055) Microsoft Visio Insecure Library Loading Remote Code Execution (2560847)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3148

Update Details

Recommendation is updated

12347 - (MS11-055) Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2560847)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3148

Update Details

Recommendation is updated

12449 - (MS11-057) Microsoft Internet Explorer Style Object Memory Corruption Remote Code Execution (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1964

Update Details

Recommendation is updated

12450 - (MS11-057) Microsoft Internet Explorer Telnet Handler Remote Code Execution (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1961

Update Details

Recommendation is updated

12454 - (MS11-057) Microsoft Internet Explorer XSLT Memory Corruption Remote Code Execution (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1963

Update Details

Recommendation is updated

12455 - (MS11-064) Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1871, CVE-2011-1965

Update Details

Recommendation is updated

12458 - (MS11-059) Microsoft Data Access Insecure Library Loading Remote Code Execution (2560656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1975

Update Details

Recommendation is updated

12459 - (MS11-060) Microsoft Visio Move Around The Block Could Allow Remote Code Execution (2560978)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1979

Update Details

Recommendation is updated

12461 - (MS11-065) Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1968

Update Details

Recommendation is updated

12462 - (MS11-060) Microsoft Visio Pstream Release Could Allow Remote Code Execution (2560978)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1972

Update Details

Recommendation is updated

12468 - (MS11-059) Vulnerability in Data Access Components Could Allow Remote Code Execution (2560656)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1975

Update Details

Recommendation is updated

12469 - (MS11-060) Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2560978)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1971, CVE-2011-1972

Update Details

Recommendation is updated

12615 - (MS11-071) Microsoft Windows Components Insecure Library Loading Remote Code Execution (2570947)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1991

Update Details

Recommendation is updated

12616 - (MS11-072) Microsoft Excel Conditional Expression Parsing Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1989

Update Details

Recommendation is updated

12617 - (MS11-072) Microsoft Excel Heap Corruption Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1988

Update Details

Recommendation is updated

12618 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1987

Update Details

Recommendation is updated

12619 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution II (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1990

Update Details

Recommendation is updated

12620 - (MS11-072) Microsoft Excel Use after Free WriteAV Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1986

Update Details

Recommendation is updated

12621 - (MS11-073) Microsoft Office Component Insecure Library Loading Remote Code Execution (2587634)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1980

Update Details

Recommendation is updated

12622 - (MS11-073) Microsoft Office Uninitialized Object Pointer Remote Code Execution (2587634)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1982

Update Details

Recommendation is updated

12624 - (MS11-070) Vulnerability In WINS Could Allow Elevation Of Privilege (2571621)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1984

Update Details

Recommendation is updated

12625 - (MS11-071) Vulnerability In Windows Components Could Allow Remote Code Execution (2570947)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1991

Update Details

Recommendation is updated

12626 - (MS11-073) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2587634)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1980, CVE-2011-1982

Update Details

Recommendation is updated

12627 - (MS11-072) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1986, CVE-2011-1987, CVE-2011-1988, CVE-2011-1989, CVE-2011-1990

Update Details

Recommendation is updated

12703 - Microsoft Windows wab32res.dll Insecure Library Loading Remote Code Execution

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3143

Update Details

Recommendation is updated

12735 - (MS11-075) Microsoft Active Accessibility Insecure Library Loading (2623699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1247

Update Details

Recommendation is updated

12736 - (MS11-076) Microsoft Windows Media Center Insecure Library Loading (2604926)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2009

Update Details

Recommendation is updated

12737 - (MS11-078) Microsoft .NET Framework Class Inheritance (2604930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1253

Update Details

Recommendation is updated

12740 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Font Library File Buffer Overrun (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2003

Update Details

Recommendation is updated

12742 - (MS11-075) Vulnerability In Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1247

Update Details

Recommendation is updated

12743 - (MS11-076) Vulnerability In Windows Media Center Could Allow Remote Code Execution (2604926)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2009

Update Details

Recommendation is updated

12744 - (MS11-077) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1985, CVE-2011-2002, CVE-2011-2003, CVE-2011-2011

Update Details

Recommendation is updated

12750 - (MS11-081) Microsoft IE Scroll Event Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1993

Update Details

Recommendation is updated

12751 - (MS11-078) Vulnerability In .NET Framework And Microsoft Silverlight Could Allow Remote Code Execution (2604930)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1253

Update Details

Recommendation is updated

12752 - (MS11-081) Microsoft IE OLEAuto32.dll Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1995

Update Details

Recommendation is updated

12753 - (MS11-081) Microsoft IE Option Element Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1996

Update Details

Recommendation is updated

12754 - (MS11-081) Microsoft IE OnLoad Event Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1997

Update Details

Recommendation is updated

12755 - (MS11-081) Microsoft IE Select Element Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1999

Update Details

Recommendation is updated

12756 - (MS11-081) Microsoft IE Body Element Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2000

Update Details

Recommendation is updated

12757 - (MS11-081) Microsoft IE Virtual Function Table Corruption Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2001

Update Details

Recommendation is updated

12763 - (MS11-081) Cumulative Security Update for Internet Explorer (2586448)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1993, CVE-2011-1995, CVE-2011-1996, CVE-2011-1997, CVE-2011-1999, CVE-2011-2000, CVE-2011-2001

Update Details

Recommendation is updated

12799 - (MS11-081) Microsoft IE Jscript9.dll Remote Code Execution (2586448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1998

Update Details

Recommendation is updated

12832 - (MS11-091) Microsoft Publisher Function Pointer Overwrite (2607702)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1508

Update Details

Recommendation is updated

12891 - (MS11-087) Microsoft Windows TrueType Font Parsing (2639417)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

12909 - (MS11-085) Microsoft Windows Mail Insecure Library Loading Remote Code Execution (2620704)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2016

Update Details

Recommendation is updated

12910 - (MS11-086) Microsoft Windows Active Directory LDAPS Authentication Bypass Privilege Escalation (2630837)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2014

Update Details

Recommendation is updated

12911 - (MS11-085) Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2016

Update Details

Recommendation is updated

12912 - (MS11-086) Vulnerability in Active Directory Could Allow Elevation of Privilege (2630837)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2014

Update Details

Recommendation is updated

13057 - (MS11-089) Microsoft Word Access Violation (2590602)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1983

Update Details

Recommendation is updated

13061 - (MS11-089) Vulnerabilities in Microsoft Word could allow for Remote Code Execution (2590602)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1983

Update Details

Recommendation is updated

13064 - (MS11-099) Microsoft Internet Explorer Insecure Library Loading (2618444)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2019

Update Details

Recommendation is updated

13067 - (MS11-090) Microsoft Time Remote Code Execution (2618451)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3397

Update Details

Recommendation is updated

13068 - (MS11-091) Microsoft Publisher Invalid Pointer (2607702)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3411

Update Details

Recommendation is updated

13069 - (MS11-091) Microsoft Publisher Memory Corruption (2607702)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3412

Update Details

Recommendation is updated

13071 - (MS11-091) Microsoft Publisher Out-of-bounds Array Index (2607702)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3410

Update Details

Recommendation is updated

13072 - (MS11-087) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

13073 - (MS11-090) Cumulative Security Update of ActiveX Kill Bits (2618451)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3397

Update Details

Recommendation is updated

13076 - (MS11-091) Vulnerabilities in Microsoft Publisher Could Allow Elevation of Privilege (2607702)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1508, CVE-2011-3410, CVE-2011-3411, CVE-2011-3412

Update Details

Recommendation is updated

13077 - (MS11-099) Cumulative Security Update for Internet Explorer (2618444)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1992, CVE-2011-2019, CVE-2011-3389, CVE-2011-3404

Update Details

Recommendation is updated

13078 - (MS11-092) Microsoft Windows Media Player DVR-MS Memory Corruption (2648048)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3401

Update Details

Recommendation is updated

13079 - (MS11-093) Microsoft Windows OLE Property (2624667)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3400

Update Details

Recommendation is updated

13080 - (MS11-094) Microsoft PowerPoint Insecure Library Loading (2639142)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3396

Update Details

Recommendation is updated

13081 - (MS11-094) Microsoft PowerPoint OfficeArt Shape RCE (2639142)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3413

Update Details

Recommendation is updated

13082 - (MS11-095) Microsoft Active Directory Buffer Overflow (2640045)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3406

Update Details

Recommendation is updated

13083 - (MS11-096) Microsoft Excel Record Memory Corruption (2640241)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3403

Update Details

Recommendation is updated

13121 - (MS12-008) Microsoft Windows GDI Access Violation (2660465)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-5046

Update Details

Recommendation is updated

13124 - (MS03-049) Microsoft Windows 2000 Workstation Service Buffer Overflow (Intrusive)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2003-0812

Update Details

Recommendation is updated

13132 - (MS03-049) Microsoft Windows XP Workstation Service Buffer Overflow (Intrusive)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2003-0812

Update Details

Recommendation is updated

13161 - (MS11-100) Microsoft .NET User Authentication Privilege Escalation (2638420)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3416

Update Details

Recommendation is updated

13162 - (MS11-100) Microsoft .NET Cached Content Privilege Escalation (2638420)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3417

Update Details

Recommendation is updated

13163 - (MS11-100) Vulnerabilities In .NET Framework Could Allow Elevation of Privilege (2638420)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3414, CVE-2011-3415, CVE-2011-3416, CVE-2011-3417

Update Details

Recommendation is updated

13183 - (MS12-004) Microsoft Media Player DirectShow Remote Code Execution (2636391)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0004

Update Details

Recommendation is updated

13184 - (MS12-005) Microsoft Windows Assembly Execution (2584146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0013

Update Details

Recommendation is updated

13185 - (MS12-004) Microsoft Media Player MIDI Remote Code Execution (2636391)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0003

Update Details

Recommendation is updated

13186 - (MS12-004) Vulnerabilities In Windows Media Could Allow Remote Code Execution (2636391)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0003, CVE-2012-0004

Update Details

Recommendation is updated

13188 - (MS12-001) Microsoft Windows Kernel SafeSEH Bypass (2644615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0001

Update Details

Recommendation is updated

13189 - (MS12-002) Microsoft Windows Object Packager Insecure Executable Launching (2603381)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0009

Update Details

Recommendation is updated

13191 - (MS12-001) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0001

Update Details

Recommendation is updated

13192 - (MS12-002) Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0009

Update Details

Recommendation is updated

13297 - (MS12-010) Microsoft IE HtmlLayout Remote Code Execution (2647516)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0011

Update Details

Recommendation is updated

13299 - (MS12-010) Microsoft IE VML Remote Code Execution (2647516)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0155

Update Details

Recommendation is updated

13300 - (MS12-014) Microsoft Indeo Codec Insecure Library Loading (2661637)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3138

Update Details

Recommendation is updated

13301 - (MS12-014) Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3138

Update Details

Recommendation is updated

13302 - (MS12-015) Microsoft Visio VSD File Format Memory Corruption I (2663510)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0019

Update Details

Recommendation is updated

13303 - (MS12-015) Microsoft Visio VSD File Format Memory Corruption II (2663510)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0020

Update Details

Recommendation is updated

13304 - (MS12-015) Microsoft Visio VSD File Format Memory Corruption III (2663510)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0136

Update Details

Recommendation is updated

13305 - (MS12-015) Microsoft Visio VSD File Format Memory Corruption IV (2663510)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0137

Update Details

Recommendation is updated

13306 - (MS12-015) Microsoft Visio VSD File Format Memory Corruption V (2663510)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0138

Update Details

Recommendation is updated

13307 - (MS12-015) Vulnerabilities in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2663510)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0019, CVE-2012-0020, CVE-2012-0136, CVE-2012-0137, CVE-2012-0138

Update Details

Recommendation is updated

13308 - (MS12-016) Microsoft .NET Framework Unmanaged Objects (2651026)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0014

Update Details

Recommendation is updated

13309 - (MS12-016) Microsoft .NET Framework Heap Corruption (2651026)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0015

Update Details

Recommendation is updated

13310 - (MS12-016) Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0014, CVE-2012-0015

Update Details

Recommendation is updated

13314 - (MS12-012) Microsoft Color Control Panel Insecure Library Loading (2643719)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-5082

Update Details

Recommendation is updated

13315 - (MS12-013) Microsoft Windows Msvcrt.dll Buffer Overflow (2654428)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0150

Update Details

Recommendation is updated

13317 - (MS12-012) Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-5082

Update Details

Recommendation is updated

13318 - (MS12-013) Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0150

Update Details

Recommendation is updated

13402 - (MS12-022) Microsoft Expression Design Insecure Library Loading (2651018)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0016

Update Details

Recommendation is updated

13403 - (MS12-022) Vulnerability in Expression Design Could Allow Remote Code Execution (2651018)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0016

Update Details

Recommendation is updated

13405 - (MS12-020) Microsoft Remote Desktop Protocol Remote Code Execution (2671387)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0002

Update Details

Recommendation is updated

13505 - (MS12-027) Microsoft Office And SQL Server MSCOMCTL.OCX Remote Code Execution (2664258)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0158

Update Details

Recommendation is updated

13506 - (MS12-027) Vulnerability In Windows Common Controls Could Allow Remote Code Execution (2664258)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0158

Update Details

Recommendation is updated

13507 - (MS12-028) Microsoft Office WPS Converter Remote Code Execution (2639185)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0177

Update Details

Recommendation is updated

13509 - (MS12-025) Microsoft Windows .NET Parameter Validation Remote Code Execution (2671605)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0163

Update Details

Recommendation is updated

13510 - (MS12-025) Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0163

Update Details

Recommendation is updated

13514 - (MS12-024) Microsoft Windows WinVerifyTrust Signature Validation (2653956)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0151

Update Details

Recommendation is updated

13516 - (MS12-023) Microsoft Internet Explorer JScript9 Remote Code Execution (2675157)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0169

Update Details

Recommendation is updated

13517 - (MS12-023) Microsoft Internet Explorer OnReadyStateChange Remote Code Execution (2675157)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0170

Update Details

Recommendation is updated

13518 - (MS12-023) Microsoft Internet Explorer SelectAll Remote Code Execution (2675157)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0171

Update Details

Recommendation is updated

13519 - (MS12-023) Microsoft Internet Explorer VML Remote Code Execution (2675157)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0172

Update Details

Recommendation is updated

13520 - (MS12-023) Cumulative Security Update for Internet Explorer (2675157)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0168, CVE-2012-0169, CVE-2012-0170, CVE-2012-0171, CVE-2012-0172

Update Details

Recommendation is updated

13521 - (MS12-024) Vulnerability in Windows Could Allow Remote Code Execution (2653956)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0151

Update Details

Recommendation is updated

13606 - (MS12-030) Microsoft Office Excel Record Parsting Type Mismatch Remote Code Execution (2663830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1847

Update Details

Recommendation is updated

13607 - (MS12-030) Microsoft Office Excel MergeCells Heap Overflow Remote Code Execution (2663830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0185

Update Details

Recommendation is updated

13608 - (MS12-030) Microsoft Office Excel SXLI Record Memory Corruption Remote Code Execution (2663830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0184

Update Details

Recommendation is updated

13609 - (MS12-030) Microsoft Office Excel Memory Corruption Using Various Modified Bytes (2663830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0143

Update Details

Recommendation is updated

13610 - (MS12-030) Microsoft Office Excel File Format Memory Corruption in OBJECTLINK Record (2663830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0142

Update Details

Recommendation is updated

13611 - (MS12-030) Microsoft Office Excel File Format Memory Corruption (2663830)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0141

Update Details

Recommendation is updated

13612 - (MS12-030) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2663830)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0141, CVE-2012-0142, CVE-2012-0143, CVE-2012-0184, CVE-2012-0185, CVE-2012-1847

Update Details

Recommendation is updated

13613 - (MS12-031) Microsoft Visio VSD File Format Memory Corruption I (2597981)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0018

Update Details

Recommendation is updated

13614 - (MS12-031) Vulnerability In Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2597981)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0018

Update Details

Recommendation is updated

13617 - (MS12-029) Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0183

Update Details

Recommendation is updated

13618 - (MS12-029) Microsoft Word RTF Mismatch Remote Code Execution (2680352)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0183

Update Details

Recommendation is updated

13622 - (MS12-034) Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

Update Details

Recommendation is updated

13624 - (MS12-034) Microsoft Silverlight Double Free Remote Code Execution (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0176

Update Details

Recommendation is updated

13625 - (MS12-034) Microsoft Windows .NET Buffer Allocation Remote Code Execution (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0162

Update Details

Recommendation is updated

13629 - (MS12-034) Microsoft Windows GDI+ Heap Overflow Remote Code Execution (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0167

Update Details

Recommendation is updated

13630 - (MS12-034) Microsoft Windows GDI+ Record Remote Code Execution (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0165

Update Details

Recommendation is updated

13631 - (MS12-034) Microsoft Windows TrueType Font Parsing II (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0159

Update Details

Recommendation is updated

13632 - (MS12-034) Microsoft Windows TrueType Font Parsing (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

13633 - (MS12-035) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0160, CVE-2012-0161

Update Details

Recommendation is updated

13634 - (MS12-035) Microsoft Windows .NET Deserialization Remote Code Execution (2696777)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0161

Update Details

Recommendation is updated

13635 - (MS12-035) Microsoft Windows .NET Serialization Remote Code Execution (2693777)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0160

Update Details

Recommendation is updated

13739 - (MS12-037) Microsoft Internet Explorer Same ID Property Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1875

Update Details

Recommendation is updated

13750 - (MS12-038) Microsoft .NET Framework Clipboard Unsafe Memory Access Remote Code Execution (2706726)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1855

Update Details

Recommendation is updated

13753 - (MS12-036) Microsoft Windows Remote Desktop Protocol Remote Code Execution (2685939)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0173

Update Details

Recommendation is updated

13754 - (MS12-036) Vulnerability In Remote Desktop Could Allow Remote Code Execution (2685939)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0173

Update Details

Recommendation is updated

13756 - (MS12-037) Microsoft Internet Explorer OnRowsInserted Event Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1881

Update Details

Recommendation is updated

13757 - (MS12-037) Microsoft Internet Explorer InsertRow Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1880

Update Details

Recommendation is updated

13758 - (MS12-037) Microsoft Internet Explorer InsertAdjacentText Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1879

Update Details

Recommendation is updated

13759 - (MS12-037) Microsoft Internet Explorer OnBeforeDeactivate Event Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1878

Update Details

Recommendation is updated

13760 - (MS12-037) Microsoft Internet Explorer Developer Toolbar Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1874

Update Details

Recommendation is updated

13761 - (MS12-037) Microsoft Internet Explorer Col Element Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1876

Update Details

Recommendation is updated

13764 - (MS12-037) Microsoft Internet Explorer Center Element Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1523

Update Details

Recommendation is updated

13766 - (MS12-037) Microsoft Internet Explorer Title Element Change Remote Code Execution (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1877

Update Details

Recommendation is updated

13767 - (MS12-037) Cumulative Security Update For Internet Explorer (2699988)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1523, CVE-2012-1858, CVE-2012-1872, CVE-2012-1873, CVE-2012-1874, CVE-2012-1875, CVE-2012-1876, CVE-2012-1877, CVE-2012-1878, CVE-2012-1879, CVE-2012-1880, CVE-2012-1881, CVE-2012-1882

Update Details

Recommendation is updated

13768 - (MS12-038) Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1855

Update Details

Recommendation is updated

13782 - (MS12-039) Microsoft Lync Insecure Library Loading Remote Code Execution (2707956)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1849

Update Details

Recommendation is updated

13784 - (MS12-039) Microsoft Windows TrueType Font Parsing II Remote Code Execution (2707956)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0159

Update Details

Recommendation is updated

13786 - (MS12-039) Microsoft Windows TrueType Font Parsing Remote Code Execution (2707956)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

13788 - (MS12-039) Vulnerabilities in Lync Could Allow Remote Code Execution (2707956)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-1849, CVE-2012-1858

Update Details

Recommendation is updated

13855 - (MS12-043) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1889

Update Details

Recommendation is updated

13856 - (MS12-044) Microsoft Internet Explorer Attribute Remove Remote Code Execution (2716177)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1524

Update Details

Recommendation is updated

13857 - (MS12-044) Microsoft Internet Explorer Cached Object Remote Code execution (2719177)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1522

Update Details

Recommendation is updated

13858 - (MS12-048) Microsoft Windows Shell Command Injection Remote Code Execution (2691442)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0175

Update Details

Recommendation is updated

13862 - (MS12-044) Cumulative Security Update for Internet Explorer (2719177)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1522, CVE-2012-1524

Update Details

Recommendation is updated

13863 - (MS12-048) Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0175

Update Details

Recommendation is updated

13873 - (MS12-045) Microsoft Data Access Components ADO Cachesize Heap Overflow Remote Code Execution(2698365)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1891

Update Details

Recommendation is updated

13875 - (MS12-045) Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1891

Update Details

Recommendation is updated

13879 - (MS12-043) Microsoft XML Core Services Uninitialized Memory Corruption Remote Code Execution (2722479)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1889

Update Details

Recommendation is updated

14011 - (MS12-052) Microsoft Internet Explorer Virtual Function Table Corruption Remote Code Execution (2722913)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2522

Update Details

Recommendation is updated

14012 - (MS12-052) Microsoft Internet Explorer Asynchronous Null Object Access Remote Code Execution (2722913)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2521

Update Details

Recommendation is updated

14013 - (MS12-052) Microsoft Internet Explorer Layout Corruption Remote Code Execution (2722913)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1526

Update Details

Recommendation is updated

14014 - (MS12-055) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2527

Update Details

Recommendation is updated

14018 - (MS12-059) Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2733918)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1888

Update Details

Recommendation is updated

14020 - (MS12-059) Microsoft Visio DXF File Format Remote Code Execution (2733918)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1888

Update Details

Recommendation is updated

14042 - (MS12-053) Microsoft Windows Remote Desktop Remote Code Execution (2723135)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2526

Update Details

Recommendation is updated

14043 - (MS12-053) Vulnerability in Remote Desktop Could Allow Remote Code Execution (2723135)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2526

Update Details

Recommendation is updated

14044 - (MS12-057) Microsoft Office CGM File Format Remote Code Execution (2731879)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2524

Update Details

Recommendation is updated

14045 - (MS12-057) Vulnerability in Microsoft Office Could Allow for Remote Code Execution (2731879)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2524

Update Details

Recommendation is updated

14046 - (MS12-060) Microsoft Office And SQL Server MSCOMCTL.OCX Remote Code Execution (2720573)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1856

Update Details

Recommendation is updated

14047 - (MS12-060) Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1856

Update Details

Recommendation is updated

14166 - (MS12-063) Cumulative Security Update for Internet Explorer

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1529, CVE-2012-2546, CVE-2012-2548, CVE-2012-2557, CVE-2012-4969

Update Details

Recommendation is updated

14207 - (MS12-064) Microsoft Word RTF Use After Free Remote Code Execution (2742319)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2528

Update Details

Recommendation is updated

14208 - (MS12-064) Microsoft Word PAPX Section Corruption Remote Code Execution (2742319)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0182

Update Details

Recommendation is updated

14211 - (MS12-065) Microsoft Works RTF Heap Memory Remote Code Execution (2754670)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2550

Update Details

Recommendation is updated

14355 - (MS12-076) Microsoft Excel SerAuxErrBar Remote Code Execution (2720184)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1885

Update Details

Recommendation is updated

14356 - (MS12-076) Microsoft Excel Memory Corruption Remote Code Exeuction (2720184)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1886

Update Details

Recommendation is updated

14357 - (MS12-076) Microsoft Excel SST Invalid Length Remote Code Execution (2720184)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1887

Update Details

Recommendation is updated

14358 - (MS12-076) Microsoft Excel Stack Overflow Remote Code Execution (2720184)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2543

Update Details

Recommendation is updated

14360 - (MS12-072) Microsoft Windows Shell Briefcase Integer Remote Code Execution I (2727528)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1527

Update Details

Recommendation is updated

14361 - (MS12-072) Microsoft Windows Shell Briefcase Integer Remote Code Execution II (2727528)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1528

Update Details

Recommendation is updated

14364 - (MS12-072) Vulnerabilities in Windows Shell Could Allow Remote Code Execution (2727528)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1527, CVE-2012-1528

Update Details

Recommendation is updated

14366 - (MS12-074) Microsoft .NET Framework Reflection Bypass Privilege Escalation (2745030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1895

Update Details

Recommendation is updated

14369 - (MS12-074) Microsoft .NET Framework Web Proxy Auto Discovery Remote Code Execution (2745030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4776

Update Details

Recommendation is updated

14370 - (MS12-074) Microsoft .NET Framework WPF Reflection Optimization Privilege Escalation (2745030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4777

Update Details

Recommendation is updated

14371 - (MS12-074) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1895, CVE-2012-1896, CVE-2012-2519, CVE-2012-4776, CVE-2012-4777

Update Details

Recommendation is updated

14378 - (MS12-071) Microsoft Internet Explorer CFormElement Remote Code Execution (2761451)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1538

Update Details

Recommendation is updated

14379 - (MS12-071) Microsoft Internet Explorer CTreeNode Remote Code Execution (2761451)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4775

Update Details

Recommendation is updated

14380 - (MS12-071) Microsoft Internet Explorer CTreePos Remote Code Execution (2761451)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1539

Update Details

Recommendation is updated

14382 - (MS12-071) Cumulative Security Update for Internet Explorer (2761451)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1538, CVE-2012-1539, CVE-2012-4775

Update Details

Recommendation is updated

14483 - (MS12-081) Microsoft Windows Filename Parsing Remote Code Execution (2758857)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4774

Update Details

Recommendation is updated

14484 - (MS12-081) Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4774

Update Details

Recommendation is updated

14485 - (MS12-079) Microsoft Word Listoverridecount Remote Code Execution (2780642)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2539

Update Details

Recommendation is updated

14486 - (MS12-079) Vulnerability in Microsoft Word Could Allow Remote Code Execution (2780642)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2539

Update Details

Recommendation is updated

14489 - (MS12-077) Microsoft Internet Explorer Improper Ref Counting User After Free Remote Code Execution (2761465)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4787

Update Details

Recommendation is updated

14490 - (MS12-077) Microsoft Internet ExplorerCMarkup User After Free Remote Code Execution (2761465)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4782

Update Details

Recommendation is updated

14491 - (MS12-077) Microsoft Internet Explorer InjectHTMLStream User After Free Remote Code Execution (2761465)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4781

Update Details

Recommendation is updated

14493 - (MS12-082) Microsoft DirectX DirectPlay Heap Overflow Remote Code Execution (2770660)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1537

Update Details

Recommendation is updated

14494 - (MS12-078) Microsoft Windows Open Type Font Parsing Remote Code Execution (2783534)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2556

Update Details

Recommendation is updated

14499 - (MS12-082) Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1537

Update Details

Recommendation is updated

14566 - (MS13-004) Microsoft .Net Framework Double Construction Privilege Escalation (2769324)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0004

Update Details

Recommendation is updated

14568 - (MS13-004) Microsoft .Net Framework WinForms Buffer Overflow Privilege Escalation (2769324)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0002

Update Details

Recommendation is updated

14569 - (MS13-004) Microsoft .Net Framework S.DS.P Buffer Overflow Privilege Escalation (2769324)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0003

Update Details

Recommendation is updated

14570 - (MS13-004) Vulnerability In .NET Framework Could Allow Elevation Of Privilege (2769324)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0001, CVE-2013-0002, CVE-2013-0003, CVE-2013-0004

Update Details

Recommendation is updated

14574 - (MS13-001) Microsoft Windows Print Spooler Remote Code Execution (2769369)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0011

Update Details

Recommendation is updated

14575 - (MS13-002) Microsoft XML Core Services Remote Code Execution (2756145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0006

Update Details

Recommendation is updated

14576 - (MS13-002) Microsoft XML Core Services Remote Code Execution II (2756145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0007

Update Details

Recommendation is updated

14578 - (MS13-001) Vulnerability in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0011

Update Details

Recommendation is updated

14579 - (MS13-002) Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0006, CVE-2013-0007

Update Details

Recommendation is updated

14617 - (MS13-008) Security Update for Internet Explorer (2799329)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4792

Update Details

Recommendation is updated

14618 - (MS13-008) Microsoft Internet Explorer CDwnBindInfo Use-After-Free Code Execution (2799329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4792

Update Details

Recommendation is updated

14648 - (MS13-019) Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0076

Update Details

Recommendation is updated

14666 - (MS13-018) Vulnerability in TCP/IP Could Allow Denial of Service (2790655)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0075

Update Details

Recommendation is updated

14671 - (MS13-009) Cumulative Security Update for Internet Explorer (2792100)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0015, CVE-2013-0018, CVE-2013-0019, CVE-2013-0020, CVE-2013-0021, CVE-2013-0022, CVE-2013-0023, CVE-2013-0024, CVE-2013-0025, CVE-2013-0026, CVE-2013-0027, CVE-2013-0028, CVE-2013-0029

Update Details

Recommendation is updated

14677 - (MS13-010) Microsoft Internet Explorer Vector Markup Language Remote Code Execution (2797052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0030

Update Details

Recommendation is updated

14678 - (MS13-011) Microsoft Windows Media Decompression Remote Code Execution (2780091)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0077

Update Details

Recommendation is updated

14684 - (MS13-020) Vulnerability in OLE Automation Could Allow Remote Code Execution (2802968)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1313

Update Details

Recommendation is updated

14693 - (MS13-020) Microsoft Windows OLE Automation Remote Code Execution (2802968)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1313

Update Details

Recommendation is updated

14695 - (MS13-009) Microsoft Internet Explorer CDispNode Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0023

Update Details

Recommendation is updated

14696 - (MS13-009) Microsoft Internet Explorer CHTML Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0029

Update Details

Recommendation is updated

14697 - (MS13-009) Microsoft Internet Explorer CMarkup Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0020

Update Details

Recommendation is updated

14698 - (MS13-009) Microsoft Internet Explorer CObjectElement Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0028

Update Details

Recommendation is updated

14699 - (MS13-009) Microsoft Internet Explorer COmWindowProxy Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0019

Update Details

Recommendation is updated

14700 - (MS13-009) Microsoft Internet Explorer CPasteCommand Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0027

Update Details

Recommendation is updated

14701 - (MS13-009) Microsoft Internet Explorer InsertElement Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0026

Update Details

Recommendation is updated

14702 - (MS13-009) Microsoft Internet Explorer LsGetTrailInfo Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0022

Update Details

Recommendation is updated

14703 - (MS13-009) Microsoft Internet Explorer PasteHTML Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0024

Update Details

Recommendation is updated

14704 - (MS13-009) Microsoft Internet Explorer SetCapture Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0018

Update Details

Recommendation is updated

14706 - (MS13-009) Microsoft Internet Explorer SLayoutRun Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0025

Update Details

Recommendation is updated

14707 - (MS13-009) Microsoft Internet Explorer Vtable Use-After-Free Remote Code Execution (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0021

Update Details

Recommendation is updated

14713 - (MS13-015) Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0073

Update Details

Recommendation is updated

14719 - (MS13-017) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1278, CVE-2013-1279, CVE-2013-1280

Update Details

Recommendation is updated

14813 - (MS13-022) Critical Vulnerability In Silverlight Could Allow Remote Code Execution (2814124)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0074

Update Details

Recommendation is updated

14814 - (MS13-022) Microsoft Silverlight Double Dereference Remote Code Execution (2814124)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0074

Update Details

Recommendation is updated

14825 - (MS13-021) Cumulative Security Update For Internet Explorer (2809289)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0087, CVE-2013-0088, CVE-2013-0089, CVE-2013-0090, CVE-2013-0091, CVE-2013-0092, CVE-2013-0093, CVE-2013-0094

Update Details

Recommendation is updated

14826 - (MS13-021) Microsoft Internet Explorer Use-After-Free Defect Remote Code Execution VIII (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0094

Update Details

Recommendation is updated

14828 - (MS13-021) Microsoft Internet Explorer Use-After-Free Defect Remote Code Execution VII (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0093

Update Details

Recommendation is updated

14829 - (MS13-021) Microsoft Internet Explorer Use-After-Free Defect Remote Code Execution VI (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0092

Update Details

Recommendation is updated

14830 - (MS13-021) Microsoft Internet Explorer Use-After-Free Defect Remote Code Execution V (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0091

Update Details

Recommendation is updated

14831 - (MS13-021) Microsoft Internet Explorer Use After Free Defect Remote Code Execution IV (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0090

Update Details

Recommendation is updated

14832 - (MS13-021) Microsoft Internet Explorer Use After Free Defect Remote Code Execution III (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0089

Update Details

Recommendation is updated

14833 - (MS13-021) Microsoft Internet Explorer Use-After-Free Defect Remote Code Execution II (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0088

Update Details

Recommendation is updated

14834 - (MS13-021) Microsoft Internet Explorer Use-After-Free Defect Remote Code Execution I (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0087

Update Details

Recommendation is updated

14843 - (MS13-024) Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0080, CVE-2013-0083, CVE-2013-0084, CVE-2013-0085

Update Details

Recommendation is updated

14849 - (MS13-021) Microsoft Internet Explorer CTreeNode Use After Free Remote Code Execution (2809289)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1288

Update Details

Recommendation is updated

14925 - (MS13-028) Cumulative Security Update for Internet Explorer (2817183)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1303, CVE-2013-1304, CVE-2013-1338

Update Details

Recommendation is updated

14926 - (MS13-028) Microsoft Internet Explorer Use After Free I Remote Code Execution (2817183)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1303

Update Details

Recommendation is updated

14927 - (MS13-028) Microsoft Internet Explorer Use After Free II Remote Code Execution (2817183)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1304

Update Details

Recommendation is updated

14928 - (MS13-036) Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege (2829996)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1283, CVE-2013-1291, CVE-2013-1292, CVE-2013-1293

Update Details

Recommendation is updated

14938 - (MS13-029) Microsoft Remote Desktop Client ActiveX Remote Code Execution (2828223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1296

Update Details

Recommendation is updated

14939 - (MS13-029) Vulnerability In Remote Desktop Client Could Allow Remote Code Execution (2828223)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15014 - (MS13-028) Microsoft Internet Explorer Use After Free III Remote Code Execution (2817183)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1338

Update Details

Recommendation is updated

15031 - (MS13-038) Security Update for Internet Explorer (2847204)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1347

Update Details

Recommendation is updated

15032 - (MS13-038) Microsoft Internet Explorer Objects In Memory Remote Code Execution (2847204)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1347

Update Details

Recommendation is updated

15037 - (MS13-043) Microsoft Office Word Shape Corruption Remote Code Execution (2830399)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1335

Update Details

Recommendation is updated

15038 - (MS13-043) Vulnerability In Microsoft Word Could Allow Remote Code Execution (2830399)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1335

Update Details

Recommendation is updated

15040 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution X (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1313

Update Details

Recommendation is updated

15041 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution IX (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1312

Update Details

Recommendation is updated

15043 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution VIII (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1311

Update Details

Recommendation is updated

15044 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution VII (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1310

Update Details

Recommendation is updated

15046 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution VI (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1309

Update Details

Recommendation is updated

15047 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution V (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1308

Update Details

Recommendation is updated

15048 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution IV (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1307

Update Details

Recommendation is updated

15049 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution III (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1306

Update Details

Recommendation is updated

15050 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution I (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0811

Update Details

Recommendation is updated

15052 - (MS13-041) Vulnerability in Lync Could Allow Remote Code Execution (2834695)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1302

Update Details

Recommendation is updated

15053 - (MS13-041) Microsoft Office Lync Remote Code Execution (2834695)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1302

Update Details

Recommendation is updated

15057 - (MS13-042) Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1316, CVE-2013-1317, CVE-2013-1318, CVE-2013-1319, CVE-2013-1320, CVE-2013-1321, CVE-2013-1322, CVE-

2013-1323, CVE-2013-1327, CVE-2013-1328, CVE-2013-1329

Update Details

Recommendation is updated

15058 - (MS13-042) Microsoft Office Publisher Negative Value Allocation Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1316

Update Details

Recommendation is updated

15059 - (MS13-042) Microsoft Office Publisher Integer Overflow Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1317

Update Details

Recommendation is updated

15060 - (MS13-042) Microsoft Office Publisher Corrupt Interface Pointer Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1318

Update Details

Recommendation is updated

15061 - (MS13-042) Microsoft Office Publisher Return Value Handling Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1319

Update Details

Recommendation is updated

15062 - (MS13-042) Microsoft Office Publisher Return Value Validation Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1321

Update Details

Recommendation is updated

15063 - (MS13-042) Microsoft Office Publisher Buffer Overflow Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1320

Update Details

Recommendation is updated

15064 - (MS13-042) Microsoft Office Publisher Invalid Range Check Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1322

Update Details

Recommendation is updated

15065 - (MS13-042) Microsoft Office Publisher Incorrect NULL Value Handling Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1323

Update Details

Recommendation is updated

15066 - (MS13-042) Microsoft Office Publisher Signed Integer Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1327

Update Details

Recommendation is updated

15067 - (MS13-042) Microsoft Office Publisher Pointer Handling Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1328

Update Details

Recommendation is updated

15068 - (MS13-042) Microsoft Office Publisher Buffer Underflow Remote Code Execution (2830397)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1329

Update Details

Recommendation is updated

15076 - (MS13-037) Microsoft Internet Explorer Use After Free Remote Code Execution II (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-2551

Update Details

Recommendation is updated

15159 - (MS13-051) Vulnerability In Microsoft Office Could Allow Remote Code Execution (2839571)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1331

Update Details

Recommendation is updated

15160 - (MS13-051) Microsoft Office Parsing Remote Code Execution (2839571)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1331

Update Details

Recommendation is updated

15162 - (MS13-047) Cumulative Security Update for Internet Explorer (2838727)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3110, CVE-2013-3111, CVE-2013-3112, CVE-2013-3113, CVE-2013-3114, CVE-2013-3116, CVE-2013-3117, CVE-2013-3118, CVE-2013-3119, CVE-2013-3120, CVE-2013-3121, CVE-2013-3122, CVE-2013-3123, CVE-2013-3124, CVE-2013-3125, CVE-2013-3126, CVE-2013-3139, CVE-2013-3141, CVE-2013-3142

Update Details

Recommendation is updated

15163 - (MS13-047) Microsoft Internet Explorer User-After-Free I Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3110

Update Details

Recommendation is updated

15164 - (MS13-049) Vulnerability In Kernel-Mode Driver Could Allow Denial Of Service (2845690)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3138

Update Details

Recommendation is updated

15165 - (MS13-047) Microsoft Internet Explorer User-After-Free III Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3112

Update Details

Recommendation is updated

15166 - (MS13-047) Microsoft Internet Explorer User-After-Free II Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3111

Update Details

Recommendation is updated

15167 - (MS13-047) Microsoft Internet Explorer User-After-Free IV Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3113

Update Details

Recommendation is updated

15168 - (MS13-047) Microsoft Internet Explorer User-After-Free V Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3114

Update Details

Recommendation is updated

15169 - (MS13-047) Microsoft Internet Explorer User-After-Free XIX Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3141

Update Details

Recommendation is updated

15170 - (MS13-047) Microsoft Internet Explorer User-After-Free VII Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3116

Update Details

Recommendation is updated

15171 - (MS13-047) Microsoft Internet Explorer User-After-Free VIII Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3117

Update Details

Recommendation is updated

15172 - (MS13-047) Microsoft Internet Explorer User-After-Free IX Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3118

Update Details

Recommendation is updated

15173 - (MS13-047) Microsoft Internet Explorer User-After-Free X Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3119

Update Details

Recommendation is updated

15174 - (MS13-047) Microsoft Internet Explorer User-After-Free XI Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3120

Update Details

Recommendation is updated

15175 - (MS13-047) Microsoft Internet Explorer User-After-Free XII Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3121

Update Details

Recommendation is updated

15176 - (MS13-047) Microsoft Internet Explorer User-After-Free XIII Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3122

Update Details

Recommendation is updated

15177 - (MS13-047) Microsoft Internet Explorer User-After-Free XIV Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3123

Update Details

Recommendation is updated

15178 - (MS13-047) Microsoft Internet Explorer User-After-Free XV Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3124

Update Details

Recommendation is updated

15179 - (MS13-047) Microsoft Internet Explorer User-After-Free XVI Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3125

Update Details

Recommendation is updated

15180 - (MS13-047) Microsoft Internet Explorer User-After-Free XVII Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3126

Update Details

Recommendation is updated

15181 - (MS13-047) Microsoft Internet Explorer User-After-Free XVIII Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3139

Update Details

Recommendation is updated

15184 - (MS13-050) Microsoft Windows Print Spooler Privilege Escalation (2839894)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1339

Update Details

Recommendation is updated

15185 - (MS13-050) Vulnerability in Windows Print Spooler Components Could Allow Elevation of Privilege (2839894)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1339

Update Details

Recommendation is updated

15190 - (MS13-047) Microsoft Internet Explorer User-After-Free XX Remote Code Execution (2838727)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3142

Update Details

Recommendation is updated

15242 - (MS13-053) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1300, CVE-2013-1340, CVE-2013-1345, CVE-2013-3129, CVE-2013-3167, CVE-2013-3172, CVE-2013-3173, CVE-2013-3660

Update Details

Recommendation is updated

15243 - (MS13-052) Microsoft Windows .NET Anonymous Method Injection Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3133

Update Details

Recommendation is updated

15244 - (MS13-052) Microsoft Windows .NET And Silverlight Array Access Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3131

Update Details

Recommendation is updated

15245 - (MS13-052) Microsoft Windows .NET And Silverlight Array Allocation Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3134

Update Details

Recommendation is updated

15246 - (MS13-057) Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (2847883)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3127

Update Details

Recommendation is updated

15247 - (MS13-052) Microsoft Windows .NET Delegate Reflection Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3132

Update Details

Recommendation is updated

15248 - (MS13-052) Microsoft .NET Framework Delegate Serialization Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3171

Update Details

Recommendation is updated

15249 - (MS13-052) Microsoft Windows Silverlight Null Pointer Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3178

Update Details

Recommendation is updated

15250 - (MS13-052) Microsoft Windows .NET And Silverlight TrueType Font Parsing Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15251 - (MS13-056) Microsoft DirectShow Arbitrary Memory Overwrite Remote Code Execution (2845187)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3174

Update Details

Recommendation is updated

15252 - (MS13-052) Vulnerabilities In .NET Framework And Silverlight Could Allow Remote Code Execution (2861561)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129, CVE-2013-3131, CVE-2013-3132, CVE-2013-3133, CVE-2013-3134, CVE-2013-3171, CVE-2013-3178

Update Details

Recommendation is updated

15255 - (MS13-057) Microsoft Windows Media Format Video Decoder Remote Code Execution (2847883)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3127

Update Details

Recommendation is updated

15256 - (MS13-054) Microsoft Windows TrueType Font Parsing Remote Code Execution (2848295)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15258 - (MS13-053) Microsoft Windows Kernel Buffer Overwrite Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3173

Update Details

Recommendation is updated

15259 - (MS13-053) Microsoft Windows Kernel Dereference Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1340

Update Details

Recommendation is updated

15260 - (MS13-056) Vulnerability In Microsoft DirectShow Could Allow Remote Code Execution (2845187)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3174

Update Details

Recommendation is updated

15261 - (MS13-054) Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15262 - (MS13-055) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3115

Update Details

Recommendation is updated

15263 - (MS13-055) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3143

Update Details

Recommendation is updated

15264 - (MS13-055) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3144

Update Details

Recommendation is updated

15266 - (MS13-055) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3145

Update Details

Recommendation is updated

15267 - (MS13-055) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3150

Update Details

Recommendation is updated

15268 - (MS13-055) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3146

Update Details

Recommendation is updated

15269 - (MS13-055) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3147

Update Details

Recommendation is updated

15270 - (MS13-055) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3148

Update Details

Recommendation is updated

15271 - (MS13-055) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3149

Update Details

Recommendation is updated

15272 - (MS13-055) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3151

Update Details

Recommendation is updated

15273 - (MS13-055) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3152

Update Details

Recommendation is updated

15274 - (MS13-055) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3153

Update Details

Recommendation is updated

15275 - (MS13-055) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3161

Update Details

Recommendation is updated

15276 - (MS13-055) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3162

Update Details

Recommendation is updated

15277 - (MS13-055) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3163

Update Details

Recommendation is updated

15278 - (MS13-055) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3164

Update Details

Recommendation is updated

15279 - (MS13-055) Cumulative Security Update for Internet Explorer (2846071)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3115, CVE-2013-3143, CVE-2013-3144, CVE-2013-3145, CVE-2013-3146, CVE-2013-3147, CVE-2013-3148, CVE-2013-3149, CVE-2013-3150, CVE-2013-3151, CVE-2013-3152, CVE-2013-3153, CVE-2013-3161, CVE-2013-3162, CVE-2013-3163, CVE-2013-3164, CVE-2013-3166, CVE-2013-3846

Update Details

Recommendation is updated

15280 - (MS13-053) Microsoft Windows Kernel Memory Allocation Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1300

Update Details

Recommendation is updated

15282 - (MS13-053) Microsoft Windows Kernel Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1345

Update Details

Recommendation is updated

15283 - (MS13-053) Microsoft Windows Kernel TrueType Font Parsing Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15284 - (MS13-053) Microsoft Windows Win32k Information Disclosure (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3167

Update Details

Recommendation is updated

15358 - (MS13-060) Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2850869)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3181

Update Details

Recommendation is updated

15367 - (MS13-064) Vulnerability In Windows NAT Driver Could Allow Denial Of Service (2849568)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3182

Update Details

Recommendation is updated

15387 - (MS13-062) Microsoft Windows Remote Procedure Call Privilege Escalation (2849470)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3175

Update Details

Recommendation is updated

15388 - (MS13-062) Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3175

Update Details

Recommendation is updated

15389 - (MS13-059) Cumulative Security Update for Internet Explorer (2862772)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3184, CVE-2013-3186, CVE-2013-3187, CVE-2013-3188, CVE-2013-3189, CVE-2013-3190, CVE-2013-3191, CVE-2013-3192, CVE-2013-3193, CVE-2013-3194, CVE-2013-3199

Update Details

Recommendation is updated

15531 - (MS13-073) Vulnerabilities In Microsoft Excel Could Allow Remote Code Execution (2858300)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1315, CVE-2013-3158, CVE-2013-3159

Update Details

Recommendation is updated

15534 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution I (2858300)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1315

Update Details

Recommendation is updated

15535 - (MS13-072) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3160, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3850, CVE-2013-3851, CVE-2013-3852, CVE-2013-3853, CVE-2013-3854, CVE-2013-3855, CVE-2013-3856, CVE-2013-3857, CVE-2013-3858

Update Details

Recommendation is updated

15537 - (MS13-069) Cumulative Security Update for Internet Explorer (2870699)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3201, CVE-2013-3202, CVE-2013-3203, CVE-2013-3204, CVE-2013-3205, CVE-2013-3206, CVE-2013-3207, CVE-2013-3208, CVE-2013-3209, CVE-2013-3845

Update Details

Recommendation is updated

15538 - (MS13-068) Microsoft Outlook Message Certificate Remote Code Execution (2756473)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3870

Update Details

Recommendation is updated

15539 - (MS13-068) Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2756473)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3870

Update Details

Recommendation is updated

15540 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution I (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3201

Update Details

Recommendation is updated

15545 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution II (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3202

Update Details

Recommendation is updated

15546 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution III (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3203

Update Details

Recommendation is updated

15547 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution IV (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3204

Update Details

Recommendation is updated

15548 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution V (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3205

Update Details

Recommendation is updated

15555 - (MS13-067) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0081, CVE-2013-1315, CVE-2013-1330, CVE-2013-3179, CVE-2013-3180, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3857, CVE-2013-3858

Update Details

Recommendation is updated

15556 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VI (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3206

Update Details

Recommendation is updated

15558 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VIII (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3208

Update Details

Recommendation is updated

15562 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution IX (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3209

Update Details

Recommendation is updated

15569 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution X (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3845

Update Details

Recommendation is updated

15574 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VII (2870699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3207

Update Details

Recommendation is updated

15588 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution I (2858300)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1315

Update Details

Recommendation is updated

15591 - (MS13-074) Microsoft Access Memory Corruption Remote Code Execution I (2848637)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3155

Update Details

Recommendation is updated

15593 - (MS13-074) Microsoft Access File Format Memory Corruption Remote Code Execution (2848637)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3156

Update Details

Recommendation is updated

15594 - (MS13-074) Microsoft Access Memory Corruption Remote Code Execution II (2848637)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3157

Update Details

Recommendation is updated

15595 - (MS13-074) Vulnerabilities in Microsoft Access Could Allow Remote Code Execution (2848637)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3155, CVE-2013-3156, CVE-2013-3157

Update Details

Recommendation is updated

15596 - (MS13-070) Microsoft Windows OLE Property Remote Code Execution (2876217)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3863

Update Details

Recommendation is updated

15597 - (MS13-070) Vulnerability in OLE Could Allow Remote Code Execution (2876217)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3863

Update Details

Recommendation is updated

15702 - (MS13-085) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3890

Update Details

Recommendation is updated

15703 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3889

Update Details

Recommendation is updated

15719 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-3889

Update Details

Recommendation is updated

15720 - (MS13-080) Cumulative Security Update for Internet Explorer (2879017)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, CVE-2013-3893, CVE-2013-3897

Update Details

Recommendation is updated

15721 - (MS13-084) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2885089)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3895

Update Details

Recommendation is updated

15724 - (MS13-083) Microsoft Windows Comctl32 Integer Overflow Remote Code Execution (2864058)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3195

Update Details

Recommendation is updated

15725 - (MS13-083) Vulnerability In Windows Common Control Library Could Allow Remote Code Execution (2864058)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3195

Update Details

Recommendation is updated

15726 - (MS13-086) Microsoft Word Memory Corruption I Remote Code Execution (2885084)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3891

Update Details

Recommendation is updated

15727 - (MS13-086) Microsoft Word Memory Corruption II Remote Code Execution (2885084)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3892

Update Details

Recommendation is updated

15728 - (MS13-082) Vulnerabilities In .NET Framework Could Allow Remote Code Execution (2878890)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3860, CVE-2013-3861

Update Details

Recommendation is updated

15729 - (MS13-086) Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2885084)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3891, CVE-2013-3892

Update Details

Recommendation is updated

15734 - (MS13-081) Microsoft Windows TrueType Font CMAP Remote Code Execution (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3894

Update Details

Recommendation is updated

15740 - (MS13-081) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3200, CVE-2013-3879, CVE-2013-3880, CVE-2013-3881, CVE-2013-3888, CVE-2013-3894

Update Details

Recommendation is updated

15751 - (MS13-081) Microsoft Windows Kernel-Mode Driver OpenType Font Parsing Remote Code Execution (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3128

Update Details

Recommendation is updated

15909 - (MS13-089) Microsoft Windows Graphics Device Interface Remote Code Execution (2876331)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3940

Update Details

Recommendation is updated

15910 - (MS13-090) Cumulative Security Update of ActiveX Kill Bits (2900986)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3918

Update Details

Recommendation is updated

15911 - (MS13-090) Microsoft ActiveX KillBits InformationCardSigninHelper Remote Code Execution (2900986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3918

Update Details

Recommendation is updated

15912 - (MS13-089) Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3940

Update Details

Recommendation is updated

15928 - (MS13-088) Cumulative Security Update for Internet Explorer (2888505)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3871, CVE-2013-3908, CVE-2013-3909, CVE-2013-3910, CVE-2013-3911, CVE-2013-3912, CVE-2013-3914, CVE-2013-3915, CVE-2013-3916, CVE-2013-3917

Update Details

Recommendation is updated

15932 - (MS13-091) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0082, CVE-2013-1324, CVE-2013-1325

Update Details

Recommendation is updated

15958 - McAfee Email Gateway GUI Remote Code Execution

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: High

CVE: CVE-2013-6349

Update Details

FASLScript is updated

16013 - (MS13-096) Vulnerability In Microsoft Graphics Component Could Allow Remote Code Execution (2908005)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3906

Update Details

Recommendation is updated

16019 - (MS13-097) Cumulative Security Update for Internet Explorer (2898785)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5045, CVE-2013-5046, CVE-2013-5047, CVE-2013-5048, CVE-2013-5049, CVE-2013-5051, CVE-2013-5052

Update Details

Recommendation is updated

16020 - (MS13-097) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5052

Update Details

Recommendation is updated

16026 - (MS13-097) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5051

Update Details

Recommendation is updated

16027 - (MS13-097) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5049

Update Details

Recommendation is updated

16028 - (MS13-097) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5048

Update Details

Recommendation is updated

16031 - (MS13-105) Microsoft Exchange MAC Disabled Remote Code Execution (2915705)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1330

Update Details

Recommendation is updated

16042 - (MS13-098) Vulnerability in Windows Could Allow Remote Code Execution (2893294)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3900

Update Details

Recommendation is updated

16043 - (MS13-099) Microsoft Windows Use After Free Remote Code Execution (2909158)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5056

Update Details

Recommendation is updated

16044 - (MS13-099) Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (2909158)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5056

Update Details

Recommendation is updated

16045 - (MS13-100) Microsoft Sharepoint Page Content Privilege Escalation (2904244)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5059

Update Details

Recommendation is updated

16047 - (MS13-102) Microsoft Windows LPC Server Buffer Overrun Privilege Escalation (2898715)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3878

Update Details

Recommendation is updated

16048 - (MS13-102) Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2898715)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3878

Update Details

Recommendation is updated

16181 - (MS13-055) Microsoft Internet Explorer CTreePos Use-After-Free Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3846

Update Details

Recommendation is updated

16212 - (MS14-002) Microsoft Windows Kernel NDProxy Component Privilege Escalation (2914368)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5065

Update Details

Recommendation is updated

16213 - (MS14-002) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2914368)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5065

Update Details

Recommendation is updated

16217 - (MS14-001) Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2916605)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0258, CVE-2014-0259, CVE-2014-0260

Update Details

Recommendation is updated

16288 - (MS14-010) Cumulative Security Update for Internet Explorer (2909921)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0267, CVE-2014-0268, CVE-2014-0269, CVE-2014-0270, CVE-2014-0271, CVE-2014-0272, CVE-2014-0273, CVE-2014-0274, CVE-2014-0275, CVE-2014-0276, CVE-2014-0277, CVE-2014-0278, CVE-2014-0279, CVE-2014-0280, CVE-2014-0281, CVE-2014-0283, CVE-2014-0284, CVE-2014-0285, CVE-2014-0286, CVE-2014-0287, CVE-2014-0288, CVE-2014-0289, CVE-2014-0290, CVE-2014-0293

Update Details

Recommendation is updated

16315 - (MS14-011) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (2928390)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0271

Update Details

Recommendation is updated

16316 - (MS14-011) Microsoft VBScript Memory Corruption Remote Code Execution (2928390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0271

Update Details

Recommendation is updated

16317 - (MS14-009) Vulnerabilities In .NET Framework Could Allow Elevation Of Privilege (2916607)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0253, CVE-2014-0257, CVE-2014-0295

Update Details

Recommendation is updated

16321 - (MS14-007) Vulnerability In Direct2D Could Allow Remote Code Execution (2912390)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0263

Update Details

Recommendation is updated

16322 - (MS14-007) Microsoft Direct2D Memory Corruption Remote Code Execution (2912390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0263

Update Details

Recommendation is updated

16366 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0281

Update Details

Recommendation is updated

16395 - (MS14-013) Vulnerability In Microsoft DirectShow Could Allow Remote Code Execution (2929961)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0301

Update Details

Recommendation is updated

16396 - (MS14-013) Microsoft DirectShow Memory Corruption Remote Code Execution (2929961)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0301

Update Details

Recommendation is updated

16405 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0324

Update Details

Recommendation is updated

16406 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0322

Update Details

Recommendation is updated

16407 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0321

Update Details

Recommendation is updated

16408 - (MS14-012) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0314

Update Details

Recommendation is updated

16409 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0313

Update Details

Recommendation is updated

16410 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0312

Update Details

Recommendation is updated

16411 - (MS14-012) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0311

Update Details

Recommendation is updated

16412 - (MS14-012) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0309

Update Details

Recommendation is updated

16413 - (MS14-012) Microsoft Internet Explorer Memory Corruption X Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0308

Update Details

Recommendation is updated

16414 - (MS14-012) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0307

Update Details

Recommendation is updated

16415 - (MS14-012) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0306

Update Details

Recommendation is updated

16416 - (MS14-012) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0305

Update Details

Recommendation is updated

16417 - (MS14-012) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0304

Update Details

Recommendation is updated

16418 - (MS14-012) Microsoft Internet Explorer Memory Corruption V Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0303

Update Details

Recommendation is updated

16419 - (MS14-012) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0302

Update Details

Recommendation is updated

16420 - (MS14-012) Microsoft Internet Explorer Memory Corruption III Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0299

Update Details

Recommendation is updated

16421 - (MS14-012) Microsoft Internet Explorer Memory Corruption II Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0298

Update Details

Recommendation is updated

16422 - (MS14-012) Microsoft Internet Explorer Memory Corruption I Remote Code Execution(2925418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0297

Update Details

Recommendation is updated

16423 - (MS14-012) Cumulative Security Update for Internet Explorer (2925418)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-

2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, CVE-2014-0322, CVE-2014-0324

Update Details

Recommendation is updated

16460 - (MS12-052) Microsoft Internet Explorer Javascript Integer Overflow Remote Code Execution (2722913)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2523

Update Details

Recommendation is updated

16461 - (MS12-056) Microsoft Windows Jscript and VBScript Remote Code Execution (2706045)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2523

Update Details

Recommendation is updated

16483 - (MS14-018) Cumulative Security Update for Internet Explorer (2950467)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0235, CVE-2014-1751, CVE-2014-1752, CVE-2014-1753, CVE-2014-1755, CVE-2014-1760

Update Details

Recommendation is updated

16490 - (MS14-020) Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (2950145)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1759

Update Details

Recommendation is updated

16492 - (MS14-017) Vulnerabilities In Microsoft Word And Office Web Apps Could Allow Remote Code Execution (2949660)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1757, CVE-2014-1758, CVE-2014-1761

Update Details

Recommendation is updated

16495 - (MS14-017) Microsoft Word RTF Files Remote Code Execution (2949660)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1761

Update Details

Recommendation is updated

16567 - (MS14-021) Microsoft Internet Explorer Use-After-Free VGX.DLL Remote Code Execution (2965111)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1776

Update Details

Recommendation is updated

16594 - (MS14-022) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2952166)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0251, CVE-2014-1754, CVE-2014-1813

Update Details

Recommendation is updated

16596 - (MS14-026) Microsoft .NET Framework TypeFilterLevel Remote Code Execution (2958732)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1806

Update Details

Recommendation is updated

16597 - (MS14-022) Microsoft SharePoint Page Content Remote Code Execution (2952166)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0251

Update Details

Recommendation is updated

16598 - (MS14-022) Microsoft SharePoint XSS Remote Code Execution (2952166)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1754

Update Details

Recommendation is updated

16599 - (MS14-022) Microsoft Web Applications Page Content Remote Code Execution (2952166)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1813

Update Details

Recommendation is updated

16613 - (MS14-029) Cumulative Security Update for Internet Explorer (2962482)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0310, CVE-2014-1815

Update Details

Recommendation is updated

16697 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2754

Update Details

Recommendation is updated

16698 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2755

Update Details

Recommendation is updated

16708 - (MS14-034) Vulnerability in Microsoft Word Could Allow Remote Code Execution (2969261)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2778

Update Details

Recommendation is updated

16711 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXVI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2756

Update Details

Recommendation is updated

16712 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXVII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2757

Update Details

Recommendation is updated

16713 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXVIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2758

Update Details

Recommendation is updated

16714 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2759

Update Details

Recommendation is updated

16715 - (MS14-035) Microsoft Internet Explorer Memory Corruption XL Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2760

Update Details

Recommendation is updated

16716 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2761

Update Details

Recommendation is updated

16717 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2763

Update Details

Recommendation is updated

16718 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2764

Update Details

Recommendation is updated

16719 - (MS14-036) Vulnerabilities In Microsoft Graphics Component Could Allow Remote Code Execution (2967487)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1817, CVE-2014-1818

Update Details

Recommendation is updated

16720 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLIV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2765

Update Details

Recommendation is updated

16721 - (MS14-036) Microsoft Unicode Scripts Processor Remote Code Execution (2967487)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1817

Update Details

Recommendation is updated

16722 - (MS14-036) Microsoft GDI+ Image Parsing Remote Code Execution (2967487)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1818

Update Details

Recommendation is updated

16723 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2766

Update Details

Recommendation is updated

16724 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLVI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2767

Update Details

Recommendation is updated

16725 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLVII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2768

Update Details

Recommendation is updated

16726 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLVIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2769

Update Details

Recommendation is updated

16727 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLIX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2770

Update Details

Recommendation is updated

16728 - (MS14-035) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0282

Update Details

Recommendation is updated

16729 - (MS14-035) Microsoft Internet Explorer Memory Corruption L Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2771

Update Details

Recommendation is updated

16730 - (MS14-035) Microsoft Internet Explorer Memory Corruption LI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2772

Update Details

Recommendation is updated

16731 - (MS14-035) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1762

Update Details

Recommendation is updated

16732 - (MS14-035) Microsoft Internet Explorer Memory Corruption LII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2773

Update Details

Recommendation is updated

16734 - (MS14-035) Microsoft Internet Explorer Memory Corruption LIV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2775

Update Details

Recommendation is updated

16735 - (MS14-035) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1769

Update Details

Recommendation is updated

16736 - (MS14-035) Microsoft Internet Explorer Memory Corruption LV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2776

Update Details

Recommendation is updated

16737 - (MS14-035) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1766

Update Details

Recommendation is updated

16739 - (MS14-035) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1770

Update Details

Recommendation is updated

16740 - (MS14-035) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1772

Update Details

Recommendation is updated

16741 - (MS14-035) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1773

Update Details

Recommendation is updated

16742 - (MS14-035) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1774

Update Details

Recommendation is updated

16743 - (MS14-035) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1775

Update Details

Recommendation is updated

16746 - (MS14-035) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1779

Update Details

Recommendation is updated

16747 - (MS14-035) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1780

Update Details

Recommendation is updated

16748 - (MS14-035) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1781

Update Details

Recommendation is updated

16749 - (MS14-035) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1782

Update Details

Recommendation is updated

16750 - (MS14-035) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1783

Update Details

Recommendation is updated

16751 - (MS14-035) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1784

Update Details

Recommendation is updated

16752 - (MS14-035) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1785

Update Details

Recommendation is updated

16753 - (MS14-035) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1786

Update Details

Recommendation is updated

16754 - (MS14-035) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1788

Update Details

Recommendation is updated

16755 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1791

Update Details

Recommendation is updated

16756 - (MS14-035) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1790

Update Details

Recommendation is updated

16757 - (MS14-035) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1789

Update Details

Recommendation is updated

16758 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1792

Update Details

Recommendation is updated

16761 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1794

Update Details

Recommendation is updated

16796 - (MS14-035) Microsoft Internet Explorer Memory Corruption LVI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2782

Update Details

Recommendation is updated

16838 - (MS14-037) Cumulative Security Update for Internet Explorer (2975687)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1763, CVE-2014-1765, CVE-2014-2783, CVE-2014-2785, CVE-2014-2786, CVE-2014-2787, CVE-2014-2788, CVE-2014-2789, CVE-2014-2790, CVE-2014-2791, CVE-2014-2792, CVE-2014-2794, CVE-2014-2795, CVE-2014-2797, CVE-2014-2798, CVE-2014-2800, CVE-2014-2801, CVE-2014-2802, CVE-2014-2803, CVE-2014-2804, CVE-2014-2806, CVE-2014-2807, CVE-2014-2809, CVE-2014-2813

Update Details

Recommendation is updated

16839 - (MS14-038) Vulnerability In Windows Journal Could Allow Remote Code Execution (2975689)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1824

Update Details

Recommendation is updated

16847 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2802

Update Details

Recommendation is updated

16848 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2801

Update Details

Recommendation is updated

16849 - (MS14-037) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2800

Update Details

Recommendation is updated

16850 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2798

Update Details

Recommendation is updated

16851 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2797

Update Details

Recommendation is updated

16852 - (MS14-037) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2795

Update Details

Recommendation is updated

16853 - (MS14-037) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2794

Update Details

Recommendation is updated

16854 - (MS14-037) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2792

Update Details

Recommendation is updated

16855 - (MS14-037) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2791

Update Details

Recommendation is updated

16856 - (MS14-037) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2790

Update Details

Recommendation is updated

16857 - (MS14-037) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2789

Update Details

Recommendation is updated

16858 - (MS14-037) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2788

Update Details

Recommendation is updated

16859 - (MS14-037) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2787

Update Details

Recommendation is updated

16860 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2804

Update Details

Recommendation is updated

16861 - (MS14-042) Vulnerability in Microsoft Service Bus Could Allow Denial Of Service (2972621)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2814

Update Details

Recommendation is updated

16863 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2806

Update Details

Recommendation is updated

16864 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2807

Update Details

Recommendation is updated

16865 - (MS14-037) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2786

Update Details

Recommendation is updated

16866 - (MS14-037) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2785

Update Details

Recommendation is updated

16867 - (MS14-037) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1765

Update Details

Recommendation is updated

16868 - (MS14-037) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1763

Update Details

Recommendation is updated

16869 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2803

Update Details

Recommendation is updated

16870 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2809

Update Details

Recommendation is updated

16874 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2813

Update Details

Recommendation is updated

16928 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1544, CVE-2014-1547, CVE-2014-1548, CVE-2014-1549, CVE-2014-1550, CVE-2014-1551, CVE-2014-1552, CVE-2014-1555, CVE-2014-1556, CVE-2014-1557, CVE-2014-1558, CVE-2014-1559, CVE-2014-1560

Update Details

FASLScript is updated

16929 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1544, CVE-2014-1547, CVE-2014-1548, CVE-2014-1549, CVE-2014-1550, CVE-2014-1551, CVE-2014-1552, CVE-2014-1555, CVE-2014-1556, CVE-2014-1557, CVE-2014-1558, CVE-2014-1559, CVE-2014-1560

Update Details

FASLScript is updated

16959 - (MS14-043) Vulnerability in Windows Media Center Could Allow Remote Code Execution (2978742)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4060

Update Details

Recommendation is updated

16966 - (MS14-051) Cumulative Security Update for Internet Explorer (2976627)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2774, CVE-2014-2784, CVE-2014-2796, CVE-2014-2808, CVE-2014-2810, CVE-2014-2811, CVE-2014-2817, CVE-2014-2818, CVE-2014-2819, CVE-2014-2820, CVE-2014-2821, CVE-2014-2822, CVE-2014-2823, CVE-2014-2824, CVE-2014-2825, CVE-2014-2826, CVE-2014-2827, CVE-2014-4050, CVE-2014-4051, CVE-2014-4052, CVE-2014-4055, CVE-2014-4056, CVE-2014-4057, CVE-2014-4058, CVE-2014-4063, CVE-2014-4067

Update Details

Recommendation is updated

16967 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4067

Update Details

Recommendation is updated

16968 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2827

Update Details

Recommendation is updated

16971 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2822

Update Details

Recommendation is updated

16972 - (MS14-051) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2821

Update Details

Recommendation is updated

16973 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4063

Update Details

Recommendation is updated

16974 - (MS14-051) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2820

Update Details

Recommendation is updated

16975 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4058

Update Details

Recommendation is updated

16976 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4057

Update Details

Recommendation is updated

16977 - (MS14-051) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4056

Update Details

Recommendation is updated

16978 - (MS14-051) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2818

Update Details

Recommendation is updated

16979 - (MS14-051) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4055

Update Details

Recommendation is updated

16980 - (MS14-051) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4052

Update Details

Recommendation is updated

16981 - (MS14-051) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4051

Update Details

Recommendation is updated

16982 - (MS14-051) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4050

Update Details

Recommendation is updated

16983 - (MS14-051) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2826

Update Details

Recommendation is updated

16984 - (MS14-051) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2811

Update Details

Recommendation is updated

16985 - (MS14-051) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2825

Update Details

Recommendation is updated

16986 - (MS14-051) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2810

Update Details

Recommendation is updated

16987 - (MS14-051) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2824

Update Details

Recommendation is updated

16988 - (MS14-051) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2808

Update Details

Recommendation is updated

16989 - (MS14-051) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2796

Update Details

Recommendation is updated

16990 - (MS14-051) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2784

Update Details

Recommendation is updated

16991 - (MS14-051) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2823

Update Details

Recommendation is updated

16992 - (MS14-051) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2774

Update Details

Recommendation is updated

17114 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31.1

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1553, CVE-2014-1562, CVE-2014-1563, CVE-2014-1564, CVE-2014-1565, CVE-2014-1567

Update Details

FASLScript is updated

17115 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1553, CVE-2014-1562, CVE-2014-1563, CVE-2014-1564, CVE-2014-1565, CVE-2014-1567

Update Details

FASLScript is updated

17225 - (MS14-057) Microsoft .NET Framework Remote Code Execution (3000414)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4121

Update Details

Recommendation is updated

17231 - (MS14-056) Cumulative Security Update for Internet Explorer (2987107)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4123, CVE-2014-4124, CVE-2014-4126, CVE-2014-4127, CVE-2014-4128, CVE-2014-4129, CVE-2014-4130, CVE-2014-4132, CVE-2014-4133, CVE-2014-4134, CVE-2014-4137, CVE-2014-4138, CVE-2014-4140, CVE-2014-4141

Update Details

Recommendation is updated

17235 - (MS14-056) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4126

Update Details

Recommendation is updated

17236 - (MS14-056) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4127

Update Details

Recommendation is updated

17237 - (MS14-056) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4128

Update Details

Recommendation is updated

17238 - (MS14-056) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4132

Update Details

Recommendation is updated

17239 - (MS14-056) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4129

Update Details

Recommendation is updated

17240 - (MS14-056) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4130

Update Details

Recommendation is updated

17241 - (MS14-056) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4133

Update Details

Recommendation is updated

17242 - (MS14-056) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4134

Update Details

Recommendation is updated

17243 - (MS14-056) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4137

Update Details

Recommendation is updated

17244 - (MS14-056) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4138

Update Details

Recommendation is updated

17245 - (MS14-056) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4141

Update Details

Recommendation is updated

17249 - (MS14-060) Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4114

Update Details

Recommendation is updated

17250 - (MS14-058) Microsoft Windows TrueType Font Parsing Remote Code Execution (3000061)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4148

Update Details

Recommendation is updated

17257 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4117

Update Details

Recommendation is updated

17259 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-4117

Update Details

Recommendation is updated

17260 - (MS14-062) Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

1354 - (MS02-072) Microsoft Windows XP MP3 Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-1327

Update Details

Recommendation is updated

1852 - (MS02-054) Microsoft Windows XP ZIP Files Long Filename Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0370, CVE-2002-1139

Update Details

Recommendation is updated

1975 - (MS03-026) Microsoft Windows RPC DCOM Buffer Overflow (Intrusive)

Category: General Vulnerability Assessment -> Instrusive -> Windows

Risk Level: High

CVE: CVE-2003-0352

Update Details

Recommendation is updated

1990 - (MS02-042) Microsoft Windows Network Connection Manager Privilege Elevation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0720

Update Details

Recommendation is updated

2064 - (MS03-041) Microsoft Windows Authenticode Verification Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0660

Update Details

Recommendation is updated

2065 - (MS03-042) Microsoft Windows Troubleshooter ActiveX Control Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0661, CVE-2003-0662, CVE-2003-0867

Update Details

Recommendation is updated

2103 - (MS04-023) Microsoft Windows Internet Explorer showHelp

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-1041, CVE-2004-0201

Update Details

Recommendation is updated

2104 - (MS04-006) Microsoft Windows WINS could allow code execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0825

Update Details

Recommendation is updated

2108 - (MS03-023) Buffer Overrun In HTML Converter patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0469

Update Details

Recommendation is updated

2121 - (MS04-007) Microsoft Windows ASN.1 could allow code execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0533, CVE-2003-0663, CVE-2003-0806, CVE-2003-0818, CVE-2003-0906, CVE-2003-0907, CVE-2003-0908, CVE-2003-0909, CVE-2003-0910

Update Details

Recommendation is updated

2268 - (MS04-013) Outlook Express IE Key

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0380

Update Details

Recommendation is updated

2560 - (MS04-022) Microsoft Windows Task Scheduler Job Overrun Patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0212

Update Details

Recommendation is updated

2800 - (MS04-037) Microsoft Windows Shell URL Command Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0214, CVE-2004-0572

Update Details

Recommendation is updated

2804 - (MS04-036) Microsoft Windows NNTP Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0574

Update Details

Recommendation is updated

2805 - (MS04-035) Microsoft Windows SMTP DNS Lookup Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0840

Update Details

Recommendation is updated

2988 - (MS04-045) Microsoft Windows WINS Server Remote Code Execution (Non-Intrusive)

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0567, CVE-2004-1080

Update Details

Recommendation is updated

3128 - (MS05-012) Microsoft Windows OLE Input Validation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0044, CVE-2005-0047

Update Details

Recommendation is updated

3133 - (MS05-008) Microsoft Internet Explorer Drag Drop

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0053, CVE-2005-0056, CVE-2005-0055, CVE-2005-0054

Update Details

Recommendation is updated

3136 - (MS05-009) Microsoft Windows Media Player 9.0 LibPNG Multiple Issues

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0597, CVE-2004-0598

Update Details

Recommendation is updated

3137 - (MS05-010) Microsoft Windows License Logging Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0050

Update Details

Recommendation is updated

3162 - (MS05-005) Microsoft Office XP Null Byte

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0848

Update Details

Recommendation is updated

3193 - (MS05-010) Microsoft Windows License Logging NT4 REMOTE

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2005-0050

Update Details

Recommendation is updated

3404 - (MS06-003) Microsoft Outlook 2003 TNEF Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0002

Update Details

Recommendation is updated

3406 - (MS05-026) Microsoft HTML Help Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1208

Update Details

Recommendation is updated

3408 - (MS06-003) Microsoft Exchange Server TNEF Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0002

Update Details

Recommendation is updated

3412 - (MS05-027) Microsoft Windows Server Message Block (SMB) Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1206

Update Details

Recommendation is updated

3442 - (MS06-003) Microsoft Outlook XP TNEF Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0002

Update Details

Recommendation is updated

3443 - (MS06-003) Microsoft Outlook 2000 TNEF Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0002

Update Details

Recommendation is updated

3606 - (MS05-036) Microsoft Windows Image Color Management Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1219

Update Details

Recommendation is updated

3796 - (MS05-043) Microsoft Windows Spooler Remote Code Execution Non-Intrusive

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2005-1984

Update Details

Recommendation is updated

3936 - (MS05-046) Microsoft Windows Netware Client Service Remote Code Execution Non-Intrusive

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2005-1985

Update Details

Recommendation is updated

4058 - (MS06-001) Microsoft Windows Windows Metafile (WMF) Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4560

Update Details

Recommendation is updated

4066 - (MS06-002) Microsoft Windows Embedded Web Fonts Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0001, CVE-2006-0010

Update Details

Recommendation is updated

4089 - (MS06-004) Microsoft Internet Explorer Cumulative Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0020

Update Details

Recommendation is updated

4091 - (MS06-006) Microsoft Windows Media Player Plugin Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0005

Update Details

Recommendation is updated

4093 - (MS06-005) Microsoft Windows Media Player Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0006

Update Details

Recommendation is updated

4174 - (MS06-012) Microsoft Excel 2000 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4176 - (MS06-012) Microsoft Excel 2003 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4177 - (MS06-012) Microsoft Excel Viewer 2003 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4178 - (MS06-012) Microsoft Outlook 2000 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4179 - (MS06-012) Microsoft Outlook 2002 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4234 - (MS06-013) Microsoft Internet Explorer Multiple Event Handler Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192, CVE-2006-1185, CVE-2006-1186, CVE-2006-1388, CVE-2006-1245, CVE-2006-1359

Update Details

Recommendation is updated

4279 - (MS06-013) Microsoft Internet Explorer createTextRange Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1359

Update Details

Recommendation is updated

4366 - (MS06-013) Microsoft Internet Explorer HTML PRE Tag Memory Corruption Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4367 - (MS06-013) Microsoft Internet Explorer Double Byte Character Parsing Memory Corruption Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1189, CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1190, CVE-2006-1191, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4368 - (MS06-013) Microsoft Internet Explorer Script Execution Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1190, CVE-2006-1185, CVE-2006-1186, CVE-2006-1188, CVE-2006-1189, CVE-2006-1191, CVE-2006-1192, CVE-2006-1245, CVE-2006-1359, CVE-2006-1388

Update Details

Recommendation is updated

4401 - (MS06-022) Microsoft ART Image Rendering Vulnerability (918439)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2378

Update Details

Recommendation is updated

4403 - (MS06-021) Microsoft Internet Explorer Exception Handling Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2218, CVE-2005-4089, CVE-2006-1303, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2382, CVE-2006-2383, CVE-2006-2384, CVE-2006-2385

Update Details

Recommendation is updated

4404 - (MS06-021) Microsoft Internet Explorer HTML Decoding Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4089, CVE-2006-1303, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-2384, CVE-2006-2385

Update Details

Recommendation is updated

4405 - (MS06-021) Microsoft Internet Explorer ActiveX Control Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2383, CVE-2005-4089, CVE-2006-1303, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-

2006-2382, CVE-2006-2384, CVE-2006-2385

Update Details

Recommendation is updated

4406 - (MS06-021) Microsoft Internet Explorer COM Object Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1303, CVE-2005-4089, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-2384, CVE-2006-2385

Update Details

Recommendation is updated

4407 - (MS06-021) Microsoft Internet Explorer Cascading Style Sheets Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4089, CVE-2006-1303, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-2384, CVE-2006-2385

Update Details

Recommendation is updated

4408 - (MS06-021) Microsoft Internet Explorer Address Bar Spoof and Information Disclosure

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2384, CVE-2005-4089, CVE-2006-1303, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-2385

Update Details

Recommendation is updated

4409 - (MS06-021) Microsoft Internet Explorer MHT Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2385, CVE-2005-4089, CVE-2006-1303, CVE-2006-1626, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-2384

Update Details

Recommendation is updated

4410 - (MS06-021) Microsoft Internet Explorer Address Bar Spoofing II

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1626, CVE-2005-4089, CVE-2006-1303, CVE-2006-1992, CVE-2006-2094, CVE-2006-2218, CVE-2006-2382, CVE-2006-2383, CVE-2006-2384, CVE-2006-2385

Update Details

Recommendation is updated

4411 - (MS06-023) Microsoft JScript Vulnerability (917344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1313

Update Details

Recommendation is updated

4413 - (MS06-028) Microsoft PowerPoint Vulnerability (916768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0022

Update Details

Recommendation is updated

4414 - (MS06-025) Microsoft RRAS Memory Corruption (911280)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2370, CVE-2006-2371

Update Details

Recommendation is updated

4415 - (MS06-025) Microsoft RRAS Registry Corruption (911280)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2370, CVE-2006-2371

Update Details

Recommendation is updated

4420 - (MS06-025) Microsoft RRAS Memory Corruption Non-intrusive (911280)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2006-2370, CVE-2006-2371

Update Details

Recommendation is updated

4445 - (MS06-035) Microsoft Server Service Mailslot Heap Overflow (917159)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1314, CVE-2006-1315

Update Details

Recommendation is updated

4447 - (MS06-036) Microsoft DHCP Client Service Vulnerability (914388)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2372

Update Details

Recommendation is updated

4448 - (MS06-037) Microsoft Excel Malformed Chart File Vulnerability (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4449 - (MS06-037) Microsoft Excel Malformed LABEL Record Vulnerability (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4450 - (MS06-037) Microsoft Excel Malformed FNGROUPCOUNT Value Vulnerability (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4451 - (MS06-037) Microsoft Excel Malformed OBJECT record Vulnerability (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4452 - (MS06-037) Microsoft Excel Malformed COLINFO Record Vulnerability (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4453 - (MS06-037) Microsoft Excel Malformed SELECTION record Vulnerability II (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4454 - (MS06-037) Microsoft Excel Malformed SELECTION record Vulnerability I (917285)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-2388, CVE-2006-3059

Update Details

Recommendation is updated

4455 - (MS06-038) Microsoft Office Property Vulnerability (917284)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1316, CVE-2006-1540, CVE-2006-2389, CVE-2006-3289

Update Details

Recommendation is updated

4456 - (MS06-038) Microsoft Office Parsing Vulnerability (917284)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1316, CVE-2006-1540, CVE-2006-2389, CVE-2006-3289

Update Details

Recommendation is updated

4457 - (MS06-038) Microsoft Office Malformed String Parsing Vulnerability (917284)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1316, CVE-2006-1540, CVE-2006-2389, CVE-2006-3289

Update Details

Recommendation is updated

4459 - (MS06-039) Microsoft Office Remote Code Execution Using a Malformed PNG Vulnerability (915384)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0007, CVE-2006-0033

Update Details

Recommendation is updated

4500 - (MS06-041) Microsoft Winsock Hostname Vulnerability (KB920683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3440, CVE-2006-3441

Update Details

Recommendation is updated

4504 - (MS06-048) Microsoft PowerPoint Malformed Records Vulnerability (KB922968)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3449, CVE-2006-3590

Update Details

Recommendation is updated

4507 - (MS06-046) Microsoft Windows Buffer Overrun in HTML Help Vulnerability (KB922616)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3357, CVE-2006-3651

Update Details

Recommendation is updated

4508 - (MS07-008) Microsoft HTML Help ActiveX Control Vulnerability (928843)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0214

Update Details

Recommendation is updated

4509 - (MS06-051) Microsoft Windows Kernel Unhandled Exception Vulnerability (KB917422)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3443, CVE-2006-3648

Update Details

Recommendation is updated

4510 - (MS06-051) Microsoft Windows Kernel User Profile Elevation of Privilege Vulnerability (KB917422)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3443, CVE-2006-3648

Update Details

Recommendation is updated

4512 - (MS06-040) Microsoft Windows Server Service Buffer Overflow (KB921883)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3439

Update Details

Recommendation is updated

4514 - (MS06-042) Microsoft Internet Explorer FTP Server Command Injection Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4515 - (MS06-042) Microsoft Internet Explorer Window Location Information Disclosure Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3640, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4516 - (MS06-042) Microsoft Internet Explorer Source Element Cross-Domain Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3639, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4517 - (MS06-042) Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3638, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4518 - (MS06-042) Microsoft Internet Explorer HTML Rendering Memory Corruption Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3637, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4519 - (MS06-042) Microsoft Internet Explorer CSS Memory Corruption Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3451, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4520 - (MS06-042) Microsoft Internet Explorer HTML Layout and Positioning Memory Corruption Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3450, CVE-2004-1166, CVE-2006-3280, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4521 - (MS06-042) Microsoft Internet Explorer Redirect Cross-Domain Information Disclosure Vulnerability (KB918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3280, CVE-2004-1166, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4522 - (MS06-040) Microsoft Windows Server Service Vulnerability No Credentials Required (KB921883)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2006-3439

Update Details

Recommendation is updated

4550 - (MS06-035) Microsoft Server Service Mailslot Heap Overflow Non-Intrusive (917159)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2006-1314, CVE-2006-1315

Update Details

Recommendation is updated

4576 - (MS06-060) Microsoft Word Malformed Stack Vulnerability (924554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3647, CVE-2006-3651, CVE-2006-4534 , CVE-2006-4693

Update Details

Recommendation is updated

4599 - (MS06-042) Microsoft Internet Explorer Long URL Buffer Overflow Vulnerability I (918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3869, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3873, CVE-2006-7029

Update Details

Recommendation is updated

4603 - (MS06-052) Microsoft Windows PGM Code Execution Vulnerability (919007)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3442

Update Details

Recommendation is updated

4610 - (MS06-042) Microsoft Internet Explorer Long URL Buffer Overflow Vulnerability II (918899)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3873, CVE-2004-1166, CVE-2006-3280, CVE-2006-3450, CVE-2006-3451, CVE-2006-3637, CVE-2006-3638, CVE-2006-3639, CVE-2006-3640, CVE-2006-3869, CVE-2006-7029

Update Details

Recommendation is updated

4616 - (MS06-067) Microsoft DirectAnimation ActiveX Controls Memory Corruption Vulnerability I (922760)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4446, CVE-2006-4687, CVE-2006-4777, CVE-2006-5884

Update Details

Recommendation is updated

4619 - (MS06-055) Microsoft Vector Markup Language Vulnerability (925486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4868, CVE-2006-3866

Update Details

Recommendation is updated

4654 - (MS06-057) Microsoft Windows Shell Remote Code Execution Vulnerability (923191)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3730, CVE-2006-4690

Update Details

Recommendation is updated

4659 - (MS06-062) Microsoft Office Improper Memory Access Vulnerability (922581)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3434, CVE-2006-3650, CVE-2006-3864, CVE-2006-3868

Update Details

Recommendation is updated

4660 - (MS06-062) Microsoft Office Malformed Chart Record Vulnerability (922581)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3434, CVE-2006-3650, CVE-2006-3864, CVE-2006-3868

Update Details

Recommendation is updated

4661 - (MS06-062) Microsoft Office Malformed Record Memory Corruption Vulnerability (922581)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3434, CVE-2006-3650, CVE-2006-3864, CVE-2006-3868

Update Details

Recommendation is updated

4662 - (MS06-062) Microsoft Office Smart Tag Parsing Vulnerability (922581)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3434, CVE-2006-3650, CVE-2006-3864, CVE-2006-3868

Update Details

Recommendation is updated

4664 - (MS06-067) Microsoft HTML Rendering Memory Corruption Vulnerability (922760)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4446, CVE-2006-4687, CVE-2006-4777, CVE-2006-5884

Update Details

Recommendation is updated

4667 - (MS06-058) Microsoft PowerPoint Malformed Object Pointer Vulnerability (924163)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3435, CVE-2006-3876, CVE-2006-3877, CVE-2006-4694, CVE-2007-0913

Update Details

Recommendation is updated

4668 - (MS06-058) Microsoft PowerPoint Malformed Data Record Vulnerability (924163)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3435, CVE-2006-3876, CVE-2006-3877, CVE-2006-4694, CVE-2007-0913

Update Details

Recommendation is updated

4669 - (MS06-058) Microsoft PowerPoint Malformed Record Memory Corruption Vulnerability (924163)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3435, CVE-2006-3876, CVE-2006-3877, CVE-2006-4694, CVE-2007-0913

Update Details

Recommendation is updated

4671 - (MS06-059) Microsoft Excel Malformed DATETIME Record Vulnerability (924164)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2387, CVE-2006-3431, CVE-2006-3867, CVE-2006-3875

Update Details

Recommendation is updated

4672 - (MS06-059) Microsoft Excel Malformed STYLE Record Vulnerability (924164)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2387, CVE-2006-3431, CVE-2006-3867, CVE-2006-3875

Update Details

Recommendation is updated

4674 - (MS06-059) Microsoft Excel Handling of Lotus 1-2-3 File Vulnerability (924164)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2387, CVE-2006-3431, CVE-2006-3867, CVE-2006-3875

Update Details

Recommendation is updated

4675 - (MS06-061) Microsoft XSLT Buffer Overrun Vulnerability (924191)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4685, CVE-2006-4686

Update Details

Recommendation is updated

4676 - (MS06-059) Microsoft Excel Malformed COLINFO Record Vulnerability (924164)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2387, CVE-2006-3431, CVE-2006-3867, CVE-2006-3875

Update Details

Recommendation is updated

4678 - (MS06-060) Microsoft Word Vulnerability (924554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3647, CVE-2006-3651, CVE-2006-4534, CVE-2006-4693

Update Details

Recommendation is updated

4680 - (MS06-060) Microsoft Word Mail Merge Vulnerability (924554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3647, CVE-2006-3651, CVE-2006-4534, CVE-2006-4693

Update Details

Recommendation is updated

4696 - (MS05-012) Microsoft Windows COM Structured Storage

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0044, CVE-2005-0047

Update Details

Recommendation is updated

4725 - (MS07-009) Microsoft Windows MDAC ActiveX Vulnerability (927779)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5559

Update Details

Recommendation is updated

4726 - (MS06-073) Microsoft Vulnerability Visual Studio 2005 Remote Code Execution (925674)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4704

Update Details

Recommendation is updated

4736 - (MS07-017) Microsoft GDI Local Elevation of Privilege Vulnerability (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5758

Update Details

Recommendation is updated

4738 - (MS06-066) Microsoft Client Service for Netware Memory Corruption Vulnerability (923980)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4688

Update Details

Recommendation is updated

4745 - (MS06-070) Microsoft Workstation Service Memory Corruption Vulnerability (924270)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4691

Update Details

Recommendation is updated

4780 - (MS07-014) Microsoft Word Malformed String Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5994

Update Details

Recommendation is updated

4783 - (MS07-014) Microsoft Word Malformed Data Structures Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6456

Update Details

Recommendation is updated

4797 - (MS06-078) Microsoft Windows Media Player ASX Vulnerability (923689)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6134, CVE-2006-4702

Update Details

Recommendation is updated

4800 - (MS07-014) Microsoft Word Count Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6561

Update Details

Recommendation is updated

4933 - (MS07-006) Microsoft Windows Shell Hardware Detection Vulnerability (928255)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0211

Update Details

Recommendation is updated

4937 - (MS07-011) Microsoft OLE Dialog Memory Corruption Vulnerability (926436)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0026

Update Details

Recommendation is updated

4940 - (MS07-014) Microsoft Word Macro Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5994, CVE-2006-6456, CVE-2006-6561, CVE-2007-0208 , CVE-2007-0209, CVE-2007-0515

Update Details

Recommendation is updated

4941 - (MS07-014) Microsoft Word Malformed Drawing Object Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5994, CVE-2006-6456, CVE-2006-6561, CVE-2007-0208, CVE-2007-0209, CVE-2007-0515

Update Details

Recommendation is updated

4943 - (MS07-016) Microsoft Internet Explorer FTP Server Response Parsing Memory Corruption Vulnerability (928090)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4697, CVE-2007-0217, CVE-2007-0219

Update Details

Recommendation is updated

5032 - (MS07-017) Microsoft Windows Animated Cursor Remote Code Execution (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215, CVE-2007-1765

Update Details

Recommendation is updated

5041 - (MS07-017) Microsoft EMF Elevation of Privilege vulnerability (925902)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1212, CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1213, CVE-2007-1215, CVE-2007-1765

Update Details

Recommendation is updated

5057 - (MS07-018) Microsoft Content Management Service Remote Code Execution Vulnerability (925939)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0938, CVE-2007-0939

Update Details

Recommendation is updated

5121 - (MS07-023) Microsoft Excel BIFF Record Vulnerability (934233)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0215, CVE-2007-1203, CVE-2007-1214

Update Details

Recommendation is updated

5122 - (MS07-023) Microsoft Excel Set Font Vulnerability (934233)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0215, CVE-2007-1203, CVE-2007-1214

Update Details

Recommendation is updated

5123 - (MS07-023) Microsoft Excel Filter Record Vulnerability (934233)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0215, CVE-2007-1203, CVE-2007-1214

Update Details

Recommendation is updated

5124 - (MS07-024) Microsoft RTF Word Parsing Vulnerability (934232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0035, CVE-2007-0870, CVE-2007-1202

Update Details

Recommendation is updated

5129 - (MS07-026) Microsoft MIME Decoding Vulnerability (931832)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0036, CVE-2007-0039, CVE-2007-0213, CVE-2007-0220, CVE-2007-0221

Update Details

Recommendation is updated

5137 - (MS07-024) Microsoft Word Document Stream Vulnerability (934232)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0035, CVE-2007-0870, CVE-2007-1202

Update Details

Recommendation is updated

5226 - (MS07-031) Microsoft Vulnerability in the Windows Schannel Security Package (935840)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2218

Update Details

Recommendation is updated

5230 - (MS07-033) Microsoft Language Pack Installation Vulnerability (933566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0218, CVE-2007-1499, CVE-2007-1750, CVE-2007-1751, CVE-2007-1752, CVE-2007-2222, CVE-2007-3027

Update Details

Recommendation is updated

5236 - (MS07-035) Microsoft Win32 API Vulnerability (935839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2219

Update Details

Recommendation is updated

5330 - (MS07-041) Microsoft IIS Memory Request Vulnerability (939373)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4360

Update Details

Recommendation is updated

5331 - (MS07-041) Microsoft IIS Memory Request Vulnerability (939373) (Intrusive)

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2005-4360

Update Details

Recommendation is updated

5413 - (MS07-042) Microsoft XML Core Services Version 3 Vulnerability (936227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2223

Update Details

Recommendation is updated

5422 - (MS07-050) Microsoft VML Buffer Overrun Vulnerability (938127)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1749

Update Details

Recommendation is updated

5427 - (MS07-042) Microsoft XML Core Services Version 4 Vulnerability (936227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2223

Update Details

Recommendation is updated

5428 - (MS07-042) Microsoft XML Core Services Version 5 Vulnerability (936227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2223

Update Details

Recommendation is updated

5429 - (MS07-042) Microsoft XML Core Services Version 6 Vulnerability (936227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2223

Update Details

Recommendation is updated

5515 - (MS07-058) Microsoft Windows RPC Authentication Vulnerability Could Allow Denial of Service (933729)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2228

Update Details

Recommendation is updated

5517 - (MS07-057) Microsoft Internet Explorer Script Error Handling Memory Corruption Vulnerability (939653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1091, CVE-2007-3826, CVE-2007-3892, CVE-2007-3893

Update Details

Recommendation is updated

5530 - (MS07-058) Microsoft Windows RPC Authentication Vulnerability Could Allow Denial of Service (933729) - No Credentials Required

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2007-2228

Update Details

Recommendation is updated

5696 - (MS08-004) Microsoft Windows Vista TCP/IP Vulnerability (946456)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0084

Update Details

Recommendation is updated

5710 - (MS08-013) Microsoft Office Malformed Object Vulnerability (947108)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0103

Update Details

Recommendation is updated

5809 - (MS08-021) Microsoft GDI stack Overflow Vulnerability (948590)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1083, CVE-2008-1087

Update Details

Recommendation is updated

6059 - (MS08-047) Microsoft IPSec Policy Information Disclosure Vulnerability (953733)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2246

Update Details

Recommendation is updated

6157 - (MS08-057) Microsoft Excel Calendar Object Validation Vulnerability (956416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3477

Update Details

Recommendation is updated

6158 - (MS08-057) Microsoft Excel File Format Parsing Vulnerability (956416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3471

Update Details

Recommendation is updated

6159 - (MS08-057) Microsoft Excel Format Parsing Vulnerability (956416)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4019

Update Details

Recommendation is updated

6190 - (MS08-067) Microsoft Windows Server Service Vulnerability (958644)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4250

Update Details

Recommendation is updated

6240 - (MS08-067) Microsoft Windows Server Service Vulnerability Intrusive (958644)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2008-4250

Update Details

Recommendation is updated

6275 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability IV (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4031

Update Details

Recommendation is updated

6276 - (MS08-072) Microsoft Word Memory Corruption Vulnerability (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4024

Update Details

Recommendation is updated

6277 - (MS08-072) Microsoft Word Memory Corruption Vulnerability II (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4837

Update Details

Recommendation is updated

6278 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability I (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4027

Update Details

Recommendation is updated

6279 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability II (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4030

Update Details

Recommendation is updated

6280 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability III (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4028

Update Details

Recommendation is updated

6281 - (MS08-072) Microsoft WordRTF Object Parsing Vulnerability (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4025

Update Details

Recommendation is updated

6282 - (MS08-072) Microsoft Word Memory Corruption Remote Code Execution (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4026

Update Details

Recommendation is updated

6301 - (MS08-078) Security Update for Internet Explorer (960714)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4844

Update Details

Recommendation is updated

6419 - (MS09-005) Microsoft Visio Memory Corruption Vulnerability - CVE-2009-0095 - (957634)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0095

Update Details

Recommendation is updated

6424 - (MS09-002) Microsoft Internet Explorer CSS Memory Corruption Vulnerability CVE-2009-0075 (961260)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0075

Update Details

Recommendation is updated

6425 - (MS09-002) Microsoft Internet Explorer CSS Memory Corruption Vulnerability CVE-2009-0076 (961260)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0076

Update Details

Recommendation is updated

6459 - (MS09-009) Microsoft Office Excel Memory Corruption Vulnerability II (968557)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0238

Update Details

Recommendation is updated

6492 - (MS09-006) Microsoft Windows Kernel Input Validation Vulnerability (958690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0081

Update Details

Recommendation is updated

6595 - (MS09-009) Microsoft Office Excel Memory Corruption Vulnerability (968557)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0100

Update Details

Recommendation is updated

6607 - (MS09-014) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (963027)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0552

Update Details

Recommendation is updated

6608 - (MS09-014) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability II (963027)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0553

Update Details

Recommendation is updated

6609 - (MS09-014) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability III (963027)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0554

Update Details

Recommendation is updated

6743 - (MS09-018) Microsoft Windows Active Directory Memory Leak Vulnerability (971055)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1139

Update Details

Recommendation is updated

6752 - (MS09-020) Microsoft IIS 5.0 WebDAV Authentication Bypass Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1122

Update Details

Recommendation is updated

6754 - (MS09-021) Microsoft Office Excel Array Indexing Memory Corruption Vulnerability (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0558

Update Details

Recommendation is updated

6755 - (MS09-021) Microsoft Office Excel Field Sensitization Memory Corruption Vulnerability (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0560

Update Details

Recommendation is updated

6756 - (MS09-021) Microsoft Office Excel Object Record Corruption Vulnerability (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0557

Update Details

Recommendation is updated

6757 - (MS09-021) Microsoft Office Excel Record Integer Overflow Vulnerability (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0561

Update Details

Recommendation is updated

6758 - (MS09-021) Microsoft Office Excel Record Pointer Corruption Vulnerability (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0549

Update Details

Recommendation is updated

6760 - (MS09-021) Microsoft Office Excel String Copy Stack-Based Overrun Vulnerability (969462)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0559

Update Details

Recommendation is updated

6771 - (MS09-027) Microsoft Office Word Buffer Overflow Vulnerability (969514)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0563

Update Details

Recommendation is updated

6772 - (MS09-027) Microsoft Office Word Buffer Overflow Vulnerability II (969514)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0565

Update Details

Recommendation is updated

6903 - (MS09-060) ATL Null String Vulnerability (973965)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2495

Update Details

Recommendation is updated

6962 - (MS09-038) Microsoft Windows Media File Malformed AVI Header Vulnerability (971557)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1545

Update Details

Recommendation is updated

7099 - (MS09-046) Microsoft Windows DHTML Editing Component ActiveX Control Vulnerability (956844)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2519

Update Details

Recommendation is updated

7106 - (MS09-048) Microsoft Windows TCP/IP Timestamps Code Execution Vulnerability (967723)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1925

Update Details

Recommendation is updated

7108 - (MS09-047) Microsoft Windows Media Header Parsing Invalid Free Vulnerability (973812)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2498

Update Details

Recommendation is updated

7109 - (MS09-047) Microsoft Windows Media Playback Memory Corruption Vulnerability (973812)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2499

Update Details

Recommendation is updated

7111 - Microsoft Windows SMB2.0 Negotiate Protocol Request Out-Of-Bounds Dereference Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-3103

Update Details

Recommendation is updated

7112 - Microsoft Windows SMB2.0 Negotiate Protocol Request Out-Of-Bounds Dereference Vulnerability

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2009-3103

Update Details

Recommendation is updated

7173 - (MS09-046) Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2519

Update Details

Recommendation is updated

7174 - (MS09-047) Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2498, CVE-2009-2499

Update Details

Recommendation is updated

7175 - (MS09-048) Vulnerabilities In Windows TCP/IP Could Allow Remote Code Execution (967723)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4609, CVE-2009-1925, CVE-2009-1926

Update Details

Recommendation is updated

7189 - (MS09-050) SMBv2 Infinite Loop Vulnerability (975517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2526

Update Details

Recommendation is updated

7196 - (MS09-054) HTML Component Handling Vulnerability (974455)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2529

Update Details

Recommendation is updated

7197 - (MS09-054) Uninitialized Memory Corruption Vulnerability II (974455)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2531

Update Details

Recommendation is updated

7328 - (MS09-063) Vulnerability in Web Service on Devices Could Allow Remote Code Execution (973565)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2512

Update Details

Recommendation is updated

7331 - (MS09-064) Vulnerability In License Logging Server Could Allow Remote Code Execution (974783)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2523

Update Details

Recommendation is updated

7333 - (MS09-066) Vulnerability In Active Directory Could Allow Denial Of Service (973309)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1928

Update Details

Recommendation is updated

7346 - (MS09-014) Cumulative Security Update For Internet Explorer (963027)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2540, CVE-2009-0550, CVE-2009-0551, CVE-2009-0552, CVE-2009-0553, CVE-2009-0554

Update Details

Recommendation is updated

7422 - (MS09-038) Vulnerabilities In Windows Media File Processing Could Allow Remote Code Execution (971557)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1545, CVE-2009-1546

Update Details

Recommendation is updated

7546 - (MS09-027) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (969514)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0563, CVE-2009-0565

Update Details

Recommendation is updated

7624 - (MS08-019) Vulnerabilities In Microsoft Visio Could Allow Remote Code Execution (949032)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1089, CVE-2008-1090

Update Details

Recommendation is updated

7636 - (MS08-004) Vulnerability In Windows TCP/IP Could Allow Denial Of Service (946456)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0084

Update Details

Recommendation is updated

7645 - (MS08-021) Vulnerabilities In GDI Could Allow Remote Code Execution (948590)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1083, CVE-2008-1087

Update Details

Recommendation is updated

7677 - (MS10-002) Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability II (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0249

Update Details

Recommendation is updated

7724 - (MS10-002) Microsoft Internet Explorer URL Validation Vulnerability (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0027

Update Details

Recommendation is updated

7725 - (MS10-002) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0244

Update Details

Recommendation is updated

7726 - (MS10-002) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability II (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0245

Update Details

Recommendation is updated

7727 - (MS10-002) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability III (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0246

Update Details

Recommendation is updated

7728 - (MS10-002) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability IV (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0247

Update Details

Recommendation is updated

7729 - (MS10-002) Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0248

Update Details

Recommendation is updated

7775 - (MS08-030) Vulnerability In Bluetooth Stack Could Allow Remote Code Execution (951376)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1453

Update Details

Recommendation is updated

7813 - (MS08-057) Vulnerabilities In Microsoft Excel Could Allow Remote Code Execution (956416)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-3471, CVE-2008-3477, CVE-2008-4019

Update Details

Recommendation is updated

7863 - (MS10-012) Microsoft Windows SMB Pathname Overflow Vulnerability (971468)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0020

Update Details

Recommendation is updated

7864 - (MS10-012) Microsoft Windows SMB Memory Corruption Vulnerability (971468)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0021

Update Details

Recommendation is updated

7865 - (MS10-012) Microsoft Windows SMB Null Pointer Vulnerability (971468)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0022

Update Details

Recommendation is updated

7866 - (MS10-012) Microsoft Windows SMB NTLM Authentication Lack of Entropy Vulnerability (971468)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0231

Update Details

Recommendation is updated

7867 - (MS10-009) Microsoft Windows ICMPv6 Router Advertisement Vulnerability (974145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0239

Update Details

Recommendation is updated

7868 - (MS10-009) Microsoft Windows Header MDL Fragmentation Vulnerability (974145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0240

Update Details

Recommendation is updated

7869 - (MS10-009) Microsoft Windows ICMPv6 Route Information Vulnerability (974145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0241

Update Details

Recommendation is updated

7870 - (MS10-009) Microsoft Windows TCP/IP Selective Acknowledgement Vulnerability (974145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0242

Update Details

Recommendation is updated

8161 - (MS08-047) Vulnerability In IPsec Policy Processing Could Allow Information Disclosure (953733)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2246

Update Details

Recommendation is updated

8298 - (MS08-072) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (957173)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4024, CVE-2008-4025, CVE-2008-4026, CVE-2008-4027, CVE-2008-4028, CVE-2008-4030, CVE-2008-4031, CVE-2008-4837

Update Details

Recommendation is updated

8394 - (MS08-078) Security Update For Internet Explorer (960714)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4844

Update Details

Recommendation is updated

8518 - (MS10-027) Microsoft Windows Media Player Remote Code Execution Vulnerability (979402)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0268

Update Details

Recommendation is updated

8527 - (MS10-028) Microsoft Visio Attribute Validation Memory Corruption Vulnerability (980094)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0254

Update Details

Recommendation is updated

8528 - (MS10-028) Microsoft Visio Index Calculation Memory Corruption Vulnerability (980094)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0256

Update Details

Recommendation is updated

8534 - (MS10-023) Microsoft Office Publisher Conversion TextBox Processing Buffer Overflow Vulnerability (981160)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0479

Update Details

Recommendation is updated

8547 - (MS10-023) Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0479

Update Details

Recommendation is updated

8830 - (MS10-031) Vulnerability In Microsoft Visual Basic For Applications Could Allow Remote Code Execution (978213)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0815

Update Details

Recommendation is updated

8832 - (MS10-031) Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0815

Update Details

Recommendation is updated

9078 - (MS10-035) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (982381)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1259

Update Details

Recommendation is updated

9079 - (MS10-035) Microsoft HTML Element Memory Corruption Vulnerability (982381)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1260

Update Details

Recommendation is updated

9080 - (MS10-035) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (982381) CVE-2010-1261

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1261

Update Details

Recommendation is updated

9081 - (MS10-035) Microsoft Internet Explorer Memory Corruption Vulnerability (982381)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1262

Update Details

Recommendation is updated

9612 - (MS10-046) Microsoft Windows Shortcut Icon Loading Remote Code Execution(2286198)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2568

Update Details

Recommendation is updated

9613 - (MS10-046) Microsoft Windows Shortcut Icon Loading Vulnerability (2286198)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2568

Update Details

Recommendation is updated

9678 - (MS10-057) Microsoft Office Excel Memory Corruption Vulnerability (2269707)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2562

Update Details

Recommendation is updated

9686 - (MS10-054) Microsoft Windows SMB Stack Exhaustion Denial Of Service (982214)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2552

Update Details

Recommendation is updated

9687 - (MS10-054) Microsoft Windows SMB Variable Validation Denial Of Service (982214)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2551

Update Details

Recommendation is updated

9692 - (MS10-051) Microsoft Windows Msxml2.XMLHTTP.3.0 Response Handling Memory Corruption Remote Code Execution (2079403)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2561

Update Details

Recommendation is updated

9712 - (MS10-058) Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1892, CVE-2010-1893

Update Details

Recommendation is updated

10039 - (MS10-065) Microsoft IIS Request Header Buffer Overflow Remote Code Execution(2267960)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2730

Update Details

Recommendation is updated

10371 - (MS10-075) Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3225

Update Details

Recommendation is updated

10372 - (MS10-075) Microsoft Windows Media Player RTSP Use After Free Remote Code Execution (2281679)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3225

Update Details

Recommendation is updated

10656 - (MS10-088) Microsoft Office PowerPoint Parsing Buffer Overflow (2293386)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2572

Update Details

Recommendation is updated

10657 - (MS10-088) Microsoft Office PowerPoint Heap Corruption Remote Code Execution (2293386)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2573

Update Details

Recommendation is updated

10661 - (MS10-087) Microsoft Office DLL Planting Vulnerability (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3337

Update Details

Recommendation is updated

10662 - (MS10-087) Microsoft Office RTF Stack Buffer Overflow (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3333

Update Details

Recommendation is updated

10664 - (MS10-087) Microsoft Office Art Drawing Records (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3334

Update Details

Recommendation is updated

10665 - (MS10-087) Microsoft Office Drawing Exception Handling (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3335

Update Details

Recommendation is updated

10666 - (MS10-087) Microsoft Office MSO Large SPID Read AV (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3336

Update Details

Recommendation is updated

10983 - (MS11-006) Windows Shell Graphics Processing Overflow (2483185)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3970

Update Details

Recommendation is updated

11755 - (MS11-019) Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0654, CVE-2011-0660

Update Details

Recommendation is updated

11769 - (MS11-033) Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0034

Update Details

Recommendation is updated

11995 - (MS11-035) Vulnerability In WINS Could Allow Remote Code Execution (2524426)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1248

Update Details

Recommendation is updated

12205 - (MS11-048) Vulnerability in SMB Server Could Allow Denial of Service (2536275)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1267

Update Details

Recommendation is updated

12211 - (MS11-045) Microsoft Excel Memory Corruption Remote Code Execution (2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1277

Update Details

Recommendation is updated

12217 - (MS11-045) Microsoft Excel Out Of Bounds WriteAV Remote Code Execution (2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1279

Update Details

Recommendation is updated

12238 - (MS11-040) Vulnerability In Threat Management Gateway Firewall Client Could Allow Remote Code Execution (KB2520426)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1889

Update Details

Recommendation is updated

12250 - (MS11-042) Vulnerabilities In Distributed File System Could Allow Remote Code Execution (2535512)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1868, CVE-2011-1869

Update Details

Recommendation is updated

12257 - (MS11-045) Microsoft Excel WriteAV Remote Code Execution (2537146)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1278

Update Details

Recommendation is updated

12348 - (MS11-056) Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1281, CVE-2011-1282, CVE-2011-1283, CVE-2011-1284, CVE-2011-1870

Update Details

Recommendation is updated

12466 - (MS11-057) Cumulative Security Update for Internet Explorer (2559049)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1257, CVE-2011-1960, CVE-2011-1961, CVE-2011-1962, CVE-2011-1963, CVE-2011-1964, CVE-2011-2383

Update Details

Recommendation is updated

12467 - (MS11-058) Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1966, CVE-2011-1970

Update Details

Recommendation is updated

12979 - (MS04-007) Microsoft Windows ASN.1 remote code execution via SMB

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2003-0818, CVE-2004-0117, CVE-2004-0119

Update Details

Recommendation is updated

12981 - (MS03-001) Microsoft Windows Locator Service REMOTE Buffer Overflow

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2003-0003

Update Details

Recommendation is updated

13084 - (MS11-092) Vulnerability in Windows Media Could Allow Remote Code Execution (2648048)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3401

Update Details

Recommendation is updated

13085 - (MS11-093) Vulnerability in OLE Could Allow Remote Code Execution (2624667)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3400

Update Details

Recommendation is updated

13086 - (MS11-094) Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2639142)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3396, CVE-2011-3413

Update Details

Recommendation is updated

13087 - (MS11-095) Vulnerability in Active Directory Could Allow Remote Code Execution (2640045)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3406

Update Details

Recommendation is updated

13088 - (MS11-096) Vulnerability in Microsoft Excel Could Allow Remote Code Execution (2640241)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3403

Update Details

Recommendation is updated

13187 - (MS12-005) Vulnerability In Microsoft Windows Could Allow Remote Code Execution (2584146)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0013

Update Details

Recommendation is updated

13292 - (MS12-008) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-5046, CVE-2012-0154

Update Details

Recommendation is updated

13295 - (MS12-010) Cumulative Security Update For Internet Explorer (2647516)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0010, CVE-2012-0011, CVE-2012-0012, CVE-2012-0155

Update Details

Recommendation is updated

13408 - (MS12-020) Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0002, CVE-2012-0152

Update Details

Recommendation is updated

13474 - (MS12-020) Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)

Category: General Vulnerability Assessment -> Instrusive -> Windows

Risk Level: High

CVE: CVE-2012-0002, CVE-2012-0152

Update Details

Recommendation is updated

13508 - (MS12-028) Vulnerability In Microsoft Office Could Allow For Remote Code Execution (2639185)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0177

Update Details

Recommendation is updated

13552 - (MS09-027) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (969514)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2009-0563, CVE-2009-0565

Update Details

Recommendation is updated

13780 - (MS12-042) Microsoft Windows BIOS ROM Corruption Privilege Escalation (2711167)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1515

Update Details

Recommendation is updated

13787 - (MS12-042) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0217, CVE-2012-1515

Update Details

Recommendation is updated

13872 - (MS12-046) Vulnerability In Microsoft Visual Basic For Applications Could Allow Remote Code Execution (2707960)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1854

Update Details

Recommendation is updated

14017 - (MS12-052) Cumulative Security Update For Internet Explorer (2722913)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1526, CVE-2012-2521, CVE-2012-2522, CVE-2012-2523

Update Details

Recommendation is updated

14019 - (MS12-054) Vulnerabilities In Windows Networking Components Could Allow Remote Code Execution (2733594)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1853, CVE-2012-1852, CVE-2012-1851, CVE-2012-1850

Update Details

Recommendation is updated

14026 - (MS12-056) Vulnerability In JScript and VBScript Engines Could Allow Remote Code Execution (2706045)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2523

Update Details

Recommendation is updated

14155 - (MS12-063) Microsoft Internet Explorer Use-After-Free exCommand Heap Stray Code Execution (2744842)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4969

Update Details

Recommendation is updated

14162 - (MS12-063) Microsoft Internet Explorer Use-After-Free OnMove Remote Code Execution (2744842)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1529

Update Details

Recommendation is updated

14163 - (MS12-063) Microsoft Internet Explorer Use-After-Free Event Listener Remote Code Execution (2744842)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2546

Update Details

Recommendation is updated

14164 - (MS12-063) Microsoft Internet Explorer Use-After-Free Layout Remote Code Execution (2744842)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2548

Update Details

Recommendation is updated

14165 - (MS12-063) Microsoft Internet Explorer Use-After-Free CloneNode Remote Code Execution (2744842)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2557

Update Details

Recommendation is updated

14210 - (MS12-064) Vulnerabilities In Microsoft Word Could Allow Remote Code Execution (2742319)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0182, CVE-2012-2528

Update Details

Recommendation is updated

14359 - (MS12-076) Vulnerabilities In Microsoft Excel Could Allow Remote Code Execution (2720184)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1885, CVE-2012-1886, CVE-2012-1887, CVE-2012-2543

Update Details

Recommendation is updated

14368 - (MS12-074) Microsoft .NET Framework Insecure Library Loading Privilege Escalation (2745030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2519

Update Details

Recommendation is updated

14492 - (MS12-077) Cumulative Security Update for Internet Explorer (2761465)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-4781, CVE-2012-4782, CVE-2012-4787

Update Details

Recommendation is updated

14564 - (MS13-007) Vulnerability in Open Data Protocol Could Allow Denial of Service (2769327)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0005

Update Details

Recommendation is updated

14565 - (MS13-007) Microsoft .NET Framework Open Data Protocol Denial Of Service (2769327)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0005

Update Details

Recommendation is updated

14672 - (MS13-010) Vulnerability In Vector Markup Language Could Allow Remote Code Execution (2797052)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0030

Update Details

Recommendation is updated

14673 - (MS13-011) Vulnerability In Media Decompression Could Allow Remote Code Execution (2780091)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0077

Update Details

Recommendation is updated

14674 - (MS13-014) Vulnerability In NFS Server Could Allow Denial of Service (2790978)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1281

Update Details

Recommendation is updated

15039 - (MS13-037) Critical Cumulative Security Update For Internet Explorer (2829530)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0811, CVE-2013-1297, CVE-2013-1306, CVE-2013-1307, CVE-2013-1308, CVE-2013-1309, CVE-2013-1310, CVE-2013-1311, CVE-2013-1312, CVE-2013-1313, CVE-2013-2551

Update Details

Recommendation is updated

15055 - (MS13-040) Microsoft .NET Framework WCF Endpoint Authentication Security Bypass (2836440)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1337

Update Details

Recommendation is updated

16566 - (MS14-021) Security Update for Internet Explorer (2965111)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1776

Update Details

Recommendation is updated

17008 - (MS14-049) Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (2962490)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1814

Update Details

Recommendation is updated

17009 - (MS14-048) Vulnerability in OneNote Could Allow Remote Code Execution (2977201)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2815

Update Details

Recommendation is updated

44004 - (MS06-070) Microsoft Workstation Service Memory Corruption Vulnerability (924270)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2006-4691

Update Details

Recommendation is updated

936 - (MS02-006) Microsoft Windows NT 4.0 SNMP Buffer Overflow (314147)

Category: General Vulnerability Assessment -> Instrusive -> Windows

Risk Level: High

CVE: CVE-2002-0053

Update Details

Recommendation is updated

1040 - Apache Chunked Encoding Transfer Memory Overwrite (Intrusive)

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2002-0392

Update Details

FASLScript is updated

1183 - (MS02-065) Microsoft Windows Remote MDAC Buffer Overflow

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2002-1142

Update Details

Recommendation is updated

1184 - (MS02-062) Microsoft IIS WebDAV Denial-of-Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0869, CVE-2002-1180, CVE-2002-1181, CVE-2002-1182

Update Details

Recommendation is updated

1497 - (MS03-005) Microsoft Windows XP Redirector Privilege Elevation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0004

Update Details

Recommendation is updated

1600 - (MS03-008) Windows Script Engine Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0010

Update Details

Recommendation is updated

1836 - (MS02-050) Microsoft Windows XP Multiple Vendor Invalid X.509 Certificate Chain

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0372, CVE-2002-0862, CVE-2002-1183, CVE-2005-0048

Update Details

Recommendation is updated

1837 - (MS02-063) Windows XP PPTP Buffer Overflow Denial-of-Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-1214

Update Details

Recommendation is updated

2016 - (MS03-030) Microsoft Windows DirectShow Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0346

Update Details

Recommendation is updated

2042 - (MS03-026) Microsoft MSBLASTER A, B, C or D Worm Detected

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0352

Update Details

Recommendation is updated

2067 - (MS03-044) Microsoft Windows Help and Support Center Buffer Overrun

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0711

Update Details

Recommendation is updated

2068 - (MS03-045) Microsoft Windows User32.dll Buffer Overrun

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0659

Update Details

Recommendation is updated

2083 - (MS03-051) Microsoft FrontPage Server Extensions Buffer Overrun Patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0822, CVE-2003-0824

Update Details

Recommendation is updated

2145 - (MS03-031) Microsoft SQL Server 2000 Named Pipe Hijacking

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2003-0230

Update Details

Recommendation is updated

2146 - (MS03-031) Microsoft SQL Server 2000 Local Procedure Call Buffer Overflow

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2003-0232

Update Details

Recommendation is updated

2236 - (MS04-007) Microsoft Windows ASN.1 remote code execution via DCOM

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2003-0818

Update Details

Recommendation is updated

2237 - (MS04-007) Microsoft Windows ASN.1 remote code execution via HTTP

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2003-0818

Update Details

Recommendation is updated

2238 - (MS04-007) Microsoft Windows ASN.1 remote code execution via SMTP

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2003-0818

Update Details

Recommendation is updated

2271 - (MS04-014) Microsoft Jet DB Engine Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0197

Update Details

Recommendation is updated

2277 - (MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via DCOM

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0123

Update Details

Recommendation is updated

2278 - (MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via HTTP

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0123

Update Details

Recommendation is updated

2280 - (MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMTP

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2004-0123

Update Details

Recommendation is updated

2335 - (MS03-017) Windows Media Player Skins Downloading Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0228

Update Details

Recommendation is updated

2408 - (MS03-026) Microsoft Windows RPC DCOM Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0352

Update Details

Recommendation is updated

2410 - (MS03-043) Microsoft Windows Messenger Service Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0717

Update Details

Recommendation is updated

2411 - (MS03-001) Microsoft Windows Locator Service Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2003-0003

Update Details

Recommendation is updated

2498 - (MS02-017) Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0151

Update Details

Recommendation is updated

2499 - (MS02-024) Authentication Flaw in Windows Debugger can Lead to Elevated Privileges

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0367

Update Details

Recommendation is updated

2566 - (MS04-020) Microsoft Windows POSIX Subsystem Privilege Escalation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0210

Update Details

Recommendation is updated

2567 - (MS04-019) Microsoft Windows Utility Manager Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0213

Update Details

Recommendation is updated

2669 - (MS04-027) Microsoft Office Word Perfect Converter Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-0573

Update Details

Recommendation is updated

3028 - (MS05-002) Microsoft Windows LoadImage API Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-1049, CVE-2004-1305, CVE-2005-0416

Update Details

Recommendation is updated

3131 - (MS05-015) Microsoft Windows Hyperlink Object Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0057

Update Details

Recommendation is updated

3132 - (MS05-007) Microsoft Windows Named Pipe Information Disclosure

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0051

Update Details

Recommendation is updated

3203 - (MS05-007) Microsoft Windows Named Pipe Information Disclosure Non Intrusive

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2005-0051

Update Details

Recommendation is updated

3299 - (MS02-032) Microsoft Windows Media Player Cumulative Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0372, CVE-2002-0373, CVE-2002-0615

Update Details

Recommendation is updated

3302 - (MS02-029) Microsoft Remote Access Service Phonebook Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2002-0366

Update Details

Recommendation is updated

3338 - (MS05-020) Microsoft Internet Explorer Cumulative Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0553, CVE-2005-0554, CVE-2005-0555

Update Details

Recommendation is updated

3340 - (MS05-016) Microsoft Windows Shell Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0063

Update Details

Recommendation is updated

3343 - (MS05-021) Microsoft Exchange Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0560

Update Details

Recommendation is updated

3411 - (MS05-028) Microsoft Web Client Service Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1207

Update Details

Recommendation is updated

3607 - (MS05-035) Microsoft Word 2000 Font Parsing Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0564

Update Details

Recommendation is updated

3608 - (MS05-035) Microsoft Word XP (2002) Font Rendering Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0564

Update Details

Recommendation is updated

3641 - (MS05-040) Microsoft Windows TAPI Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0058

Update Details

Recommendation is updated

3888 - (MS05-052) Microsoft Internet Explorer Cumulative Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-2127

Update Details

Recommendation is updated

3889 - (MS05-053) Microsoft Windows Enhanced Metafile EMF Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0803, CVE-2005-2123, CVE-2005-2124

Update Details

Recommendation is updated

3891 - (MS05-051) Microsoft Windows COM+ Memory Structures

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1978, CVE-2005-1979, CVE-2005-1980, CVE-2005-2119

Update Details

Recommendation is updated

3892 - (MS05-048) Microsoft Collaboration Data Objects Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1987

Update Details

Recommendation is updated

3897 - (MS05-048) Microsoft Exchange Collaboration Data Objects Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1987

Update Details

Recommendation is updated

3939 - (MS05-051) Microsoft COM+/MSDTC Remote Code Execution Nonintrusive

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2005-1978, CVE-2005-1979, CVE-2005-1980, CVE-2005-2119

Update Details

Recommendation is updated

4087 - (MS06-009) Microsoft Windows Korean Input Privilege Escalation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0008

Update Details

Recommendation is updated

4088 - (MS06-009) Microsoft Office 2003 Korean Input Method Editor (IME) Privilege Escalation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0008

Update Details

Recommendation is updated

4175 - (MS06-012) Microsoft Excel 2002 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4180 - (MS06-012) Microsoft PowerPoint 2000 Malformed Routing Slip

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4181 - (MS06-012) Microsoft PowerPoint 2002 Malformed Routing Slip

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4182 - (MS06-012) Microsoft Word 2000 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4183 - (MS06-012) Microsoft Word 2002 Multiple Vulnerabilities

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-4131, CVE-2006-0009, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031

Update Details

Recommendation is updated

4363 - (MS06-017) Microsoft FrontPage Server Extensions Cross Site Scripting

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0015

Update Details

Recommendation is updated

4371 - (MS06-014) Microsoft Data Access Components (MDAC) Function Could Allow Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0003

Update Details

Recommendation is updated

4377 - (MS06-019) Microsoft Exchange Calendar Parsing Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0027

Update Details

Recommendation is updated

4380 - (MS06-018) Microsoft Windows MSDTC Invalid Memory Access DoS Vulnerability (Credentials)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-0034, CVE-2006-1184, CVE-2006-1299

Update Details

Recommendation is updated

4381 - (MS06-018) Microsoft Windows MSDTC Stack Overflow DoS Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1184

Update Details

Recommendation is updated

4382 - (MS06-018) Microsoft Windows MSDTC Invalid Memory Access DoS Vulnerability (No Credentials)

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-2006-0034, CVE-2006-1184, CVE-2006-1299

Update Details

Recommendation is updated

4390 - (MS06-027) Microsoft Word Code Execution Vulnerability (917336)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2492

Update Details

Recommendation is updated

4446 - (MS06-035) Microsoft Server Service SMB Information Disclosure Vulnerability (917159)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-1314, CVE-2006-1315

Update Details

Recommendation is updated

4460 - (MS06-035) Microsoft Server Service SMB Information Disclosure Vulnerability Non-Intrusive (917159)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2006-1314, CVE-2006-1315

Update Details

Recommendation is updated

4480 - (MS06-048) Microsoft PowerPoint Mso.dll Vulnerability (KB922968)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3449, CVE-2006-3590

Update Details

Recommendation is updated

4506 - (MS06-049) Microsoft Windows 2000 Kernel Buffer Overflow (KB920958)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3444

Update Details

Recommendation is updated

4673 - (MS06-061) Microsoft XML Core Services Vulnerability (924191)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4685, CVE-2006-4686

Update Details

Recommendation is updated

4677 - (MS06-065) Microsoft Object Packager Dialogue Spoofing Vulnerability (924496)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4692

Update Details

Recommendation is updated

4695 - (MS05-002) Microsoft Windows Kernel Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2004-1049, CVE-2004-1305, CVE-2005-0416

Update Details

Recommendation is updated

4702 - (MS05-051) Microsoft Windows MSDTC Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1978, CVE-2005-1979, CVE-2005-1980, CVE-2005-2119

Update Details

Recommendation is updated

4703 - (MS05-051) Microsoft Windows MSDTC Distributed Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1978, CVE-2005-1979, CVE-2005-1980, CVE-2005-2119

Update Details

Recommendation is updated

4704 - (MS05-051) Microsoft Windows MSDTC Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-1978, CVE-2005-1979, CVE-2005-1980, CVE-2005-2119

Update Details

Recommendation is updated

4705 - (MS05-053) Microsoft Windows Graphics Rendering Engine Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0803, CVE-2005-2123, CVE-2005-2124

Update Details

Recommendation is updated

4706 - (MS05-053) Microsoft Windows Metafile WMF Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2005-0803, CVE-2005-2123, CVE-2005-2124

Update Details

Recommendation is updated

4729 - (MS06-071) Microsoft XML Core Services Remote Code Execution Vulnerability (928088)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5745

Update Details

Recommendation is updated

4737 - (MS06-069) Microsoft Macromedia Flash Player Unspecified allowScriptAccess Bypass (923789)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4640, CVE-2006-3014, CVE-2006-3311, CVE-2006-3587, CVE-2006-3588

Update Details

Recommendation is updated

4739 - (MS06-066) Microsoft Windows Netware Driver Denial of Service Vulnerability (923980)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4689

Update Details

Recommendation is updated

4740 - (MS06-068) Microsoft Agent Memory Corruption Vulnerability (920213)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3445

Update Details

Recommendation is updated

4741 - (MS06-069) Microsoft Excel Macromedia Flash ActiveX Object Code Execution (923789)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3014, CVE-2006-3311, CVE-2006-3587, CVE-2006-3588, CVE-2006-4640

Update Details

Recommendation is updated

4742 - (MS06-069) Microsoft Macromedia Flash Player Long String SWF Buffer Overflow (923789)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3311, CVE-2006-3014, CVE-2006-3587, CVE-2006-3588, CVE-2006-4640

Update Details

Recommendation is updated

4743 - (MS06-069) Microsoft Macromedia Flash Player Malformed SWF Improper Memory Access (923789)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3587, CVE-2006-3014, CVE-2006-3311, CVE-2006-3588, CVE-2006-4640

Update Details

Recommendation is updated

4744 - (MS06-069) Microsoft Macromedia Flash Player Compressed SWF Denial of Service (923789)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3588, CVE-2006-3014, CVE-2006-3311, CVE-2006-3587, CVE-2006-4640

Update Details

Recommendation is updated

4793 - (MS06-075) Microsoft File Manifest Corruption Vulnerability (926255)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5585

Update Details

Recommendation is updated

4794 - (MS06-076) Microsoft Windows Address Book Contact Record Vulnerability (923694)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2386

Update Details

Recommendation is updated

4795 - (MS06-077) Microsoft RIS Writable Path Vulnerability (926121)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5584

Update Details

Recommendation is updated

4796 - (MS06-078) Microsoft Windows Media Player WMVCORE Vulnerability (923689)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-4702, CVE-2006-6134

Update Details

Recommendation is updated

4805 - (MS06-077) Microsoft RIS Writable Path Vulnerability (926121) - No Credentials Required

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5584

Update Details

Recommendation is updated

4837 - (MS07-021) Microsoft CSRSS DoS Vulnerability (930178)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6696, CVE-2006-6797, CVE-2007-1209

Update Details

Recommendation is updated

4935 - (MS07-007) Microsoft Windows Image Acquisition Vulnerability (927802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0210

Update Details

Recommendation is updated

5059 - (MS07-019) Microsoft UPnP Memory Corruption Vulnerability (931261)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1204

Update Details

Recommendation is updated

5061 - (MS07-021) Microsoft CSRSS Local Elevation of Privilege Vulnerability (930178)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6696, CVE-2006-6797, CVE-2007-1209

Update Details

Recommendation is updated

5062 - (MS07-022) Microsoft Local Kernel EOP Vulnerability (931784)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-1206, CVE-2007-1973

Update Details

Recommendation is updated

5519 - (MS07-062) Microsoft DNS Spoofing Attack Vulnerability (941672)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3898

Update Details

Recommendation is updated

5626 - (MS07-066) Microsoft Windows Kernel Vulnerability (943078)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5350

Update Details

Recommendation is updated

5697 - (MS08-005) Microsoft File Change Notification Vulnerability (942831)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0074

Update Details

Recommendation is updated

5805 - (MS08-025) Microsoft Windows Kernel Vulnerability (941693)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1084

Update Details

Recommendation is updated

5811 - (MS08-020) Microsoft DNS Client Spoofing Vulnerability (945553)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0087

Update Details

Recommendation is updated

5919 - (MS08-030) Microsoft Bluetooth Vulnerability (951376)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1453

Update Details

Recommendation is updated

5926 - (MS08-035) Microsoft Active Directory LDAP Vulnerability (953235)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1445

Update Details

Recommendation is updated

5927 - (MS08-036) Microsoft PGM Invalid Length Vulnerability (950762)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1440 , CVE-2008-1441

Update Details

Recommendation is updated

5928 - (MS08-036) Microsoft PGM Malformed Fragment Vulnerability (950762)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1441, CVE-2008-1440

Update Details

Recommendation is updated

5995 - (MS08-037) Microsoft DNS Insufficient Socket Entropy Vulnerability (953230)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1447

Update Details

Recommendation is updated

6060 - (MS08-048) Microsoft URL Parsing Cross Domain Information Disclosure Vulnerability (951066)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1448

Update Details

Recommendation is updated

6174 - (MS08-058) Microsoft Window Location Property Cross-Domain Information Disclosure Vulnerability (956390)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2947

Update Details

Recommendation is updated

6266 - (MS08-070) Microsoft Charts Control Memory Corruption Vulnerability (932349)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4256

Update Details

Recommendation is updated

6268 - (MS08-070) Microsoft FlexGrid Control Memory Corruption Vulnerability (932349)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4253

Update Details

Recommendation is updated

6269 - (MS08-070) Microsoft Hierarchical FlexGrid Control Memory Corruption Vulnerability (932349)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4254

Update Details

Recommendation is updated

6285 - (MS08-073) Microsoft Internet Explorer Parameter Validation Memory Corruption Vulnerability (958215)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4258

Update Details

Recommendation is updated

6286 - (MS08-073) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (958215)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4260

Update Details

Recommendation is updated

6294 - (MS08-077) Microsoft Office Sharepoint Access Control Vulnerability (957175)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4032

Update Details

Recommendation is updated

6495 - (MS09-007) Microsoft Windows SChannel Spoofing Vulnerability (960225)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0085

Update Details

Recommendation is updated

6750 - (MS09-019) Microsoft Internet Explorer Race Condition Cross-Domain Information Disclosure Vulnerability (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-3091

Update Details

Recommendation is updated

6961 - (MS09-038) Microsoft Windows Media File AVI Integer Overflow Vulnerability (971557)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1546

Update Details

Recommendation is updated

7105 - (MS09-048) Microsoft Windows TCP/IP Zero Window Size Vulnerability (967723)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4609

Update Details

Recommendation is updated

7199 - (MS09-056) Integer Overflow in X.509 Object Identifiers Vulnerability (974571)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2511

Update Details

Recommendation is updated

7227 - (MS09-058) Vulnerabilities In Windows Kernel Could Allow Elevation of Privilege (971486)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2515, CVE-2009-2516, CVE-2009-2517

Update Details

Recommendation is updated

7316 - (MS09-065) Win32k NULL Pointer Dereferencing Vulnerability (969947)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1127

Update Details

Recommendation is updated

7317 - (MS09-065) Win32k Insufficient Data Validation Vulnerability (969947)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2513

Update Details

Recommendation is updated

7327 - (MS09-066) Vulnerability in Active Directory Could Allow Denial of Service (973309)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1928

Update Details

Recommendation is updated

7381 - (MS09-020) Vulnerabilities In Internet Information Services (IIS) Could Allow Elevation Of Privilege (970483)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1122, CVE-2009-1535

Update Details

Recommendation is updated

7414 - (MS09-007) Vulnerability In SChannel Could Allow Spoofing (960225)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0085

Update Details

Recommendation is updated

7627 - (MS08-003) Vulnerability In Active Directory Could Allow Denial Of Service (946538)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0088

Update Details

Recommendation is updated

7648 - (MS08-035) Vulnerability In Active Directory Could Allow Denial of Service (953235)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1445

Update Details

Recommendation is updated

7681 - (MS08-061)Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (954211)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2250, CVE-2008-2251, CVE-2008-2252

Update Details

Recommendation is updated

7704 - (MS08-005) Vulnerability In Internet Information Services Could Allow Elevation Of Privilege (942831)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-0074

Update Details

Recommendation is updated

7732 - (MS08-025) Vulnerability In Windows Kernel Could Allow Elevation Of Privilege (941693)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1084

Update Details

Recommendation is updated

7814 - (MS08-034) Vulnerability In WINS Could Allow Elevation Of Privilege (948745)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1451

Update Details

Recommendation is updated

7860 - (MS10-015) Windows Kernel Exception Handler Vulnerability (977165)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0232

Update Details

Recommendation is updated

7861 - (MS10-015) Windows Kernel Double Free Vulnerability (977165)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0233

Update Details

Recommendation is updated

7889 - (MS10-015) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0232, CVE-2010-0233

Update Details

Recommendation is updated

7944 - (MS08-041) Vulnerability In The ActiveX Control For The Snapshot Viewer For Microsoft Access Could Allow Remote Code Execution (

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2463

Update Details

Recommendation is updated

8214 - (MS08-048) Security Update For Outlook Express And Windows Mail (951066)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1448

Update Details

Recommendation is updated

8393 - (MS08-077) Vulnerability In Microsoft Office SharePoint Server Could Cause Elevation Of Privilege (957175)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4032

Update Details

Recommendation is updated

8535 - (MS10-022) Microsoft VBScript Help Keypress Vulnerability (981169)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0483

Update Details

Recommendation is updated

8545 - (MS10-021) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0234, CVE-2010-0235, CVE-2010-0236, CVE-2010-0237, CVE-2010-0238, CVE-2010-0481, CVE-2010-0482, CVE-2010-0810

Update Details

Recommendation is updated

9064 - (MS10-037) Vulnerability In The OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0819

Update Details

Recommendation is updated

9680 - (MS10-058) Microsoft Windows IPv6 Memory Corruption Denial Of Service (978886)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1892

Update Details

Recommendation is updated

9694 - (MS10-048) Microsoft Windows Win32k Window Creation Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1897

Update Details

Recommendation is updated

9695 - (MS10-048) Microsoft Windows Win32k User Input Validation Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1896

Update Details

Recommendation is updated

9696 - (MS10-048) Microsoft Windows Win32k Exception Handling Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1894

Update Details

Recommendation is updated

9715 - (MS10-047) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1888, CVE-2010-1889, CVE-2010-1890

Update Details

Recommendation is updated

9722 - (MS10-048) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1887, CVE-2010-1894, CVE-2010-1895, CVE-2010-1896, CVE-2010-1897

Update Details

Recommendation is updated

10313 - (MS10-086) Vulnerability in Windows Shared Cluster Disks Could Allow Tampering (2294255)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3223

Update Details

Recommendation is updated

10314 - (MS10-086) Microsoft Windows Permissions on New Cluster Disks Information Disclosure (2294255)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3223

Update Details

Recommendation is updated

10317 - (MS10-085) Vulnerability in SChannel Could Allow Denial of Service (2207566)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3229

Update Details

Recommendation is updated

10318 - (MS10-085) Microsoft Windows TLSv1 Denial of Service (2207566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3229

Update Details

Recommendation is updated

10320 - (MS10-084) Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3222

Update Details

Recommendation is updated

10364 - (MS10-081) Microsoft Windows Explorer Comctl32 Heap Overflow Remote Code Execution (2296011)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2746

Update Details

Recommendation is updated

10376 - (MS10-078) Vulnerabilities in the OpenType Font Format Driver Could Allow Elevation of Privilege (2279986)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2740, CVE-2010-2741

Update Details

Recommendation is updated

10377 - (MS10-078) Microsoft Windows OpenType Font Parsing Privilege Escalation (2279986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2740

Update Details

Recommendation is updated

10378 - (MS10-078) Microsoft Windows OpenType Font Validation Remote Code Execution (2279986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2741

Update Details

Recommendation is updated

10751 - (MS10-092) Microsoft Windows Task Scheduler Could Allow Elevation of Privilege (2305420)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3338

Update Details

Recommendation is updated

10773 - (MS11-011) Windows Kernel Improper Data Validation (2393802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4398

Update Details

Recommendation is updated

10857 - (MS10-092) Vulnerability In Task Scheduler Could Allow Elevation of Privilege (2305420)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3338

Update Details

Recommendation is updated

10869 - (MS10-098) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3939, CVE-2010-3940, CVE-2010-3941, CVE-2010-3942, CVE-2010-3943, CVE-2010-3944

Update Details

Recommendation is updated

10885 - (MS10-091) Microsoft Windows OpenType Font Double Free Vulnerability (2296199)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3957

Update Details

Recommendation is updated

10886 - (MS10-091) Microsoft Windows OpenType CMAP Table Vulnerability (2296199)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3959

Update Details

Recommendation is updated

10898 - (MS10-098) Microsoft Windows Win32k Buffer Overflow Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2739, CVE-2010-3939

Update Details

Recommendation is updated

10899 - (MS10-098) Microsoft Windows Win32k Buffer Overflow Could Allow Elevation Of Privilege CVE-2010-3940 (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3940

Update Details

Recommendation is updated

10900 - (MS10-098) Microsoft Windows Win32k Double Free Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3941

Update Details

Recommendation is updated

10901 - (MS10-098) Microsoft Windows Win32k WriteAV Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3942

Update Details

Recommendation is updated

10902 - (MS10-098) Microsoft Windows Win32k Cursor Linking Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3943

Update Details

Recommendation is updated

10903 - (MS10-098) Microsoft Windows Win32k Memory Corruption Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3944

Update Details

Recommendation is updated

10905 - (MS10-099) Microsoft Windows Routing and Remote Access Could Allow Elevation of Privilege (2440591)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3963

Update Details

Recommendation is updated

10906 - (MS10-100) Microsoft Windows Consent User Interface Could Allow Elevation of Privilege (2442962)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3961

Update Details

Recommendation is updated

10909 - (MS10-104) Microsoft Windows SharePoint Could Allow Remote Code Execution (KB2455005)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3964

Update Details

Recommendation is updated

10910 - (MS10-099) Vulnerability In Routing and Remote Access Could Allow Elevation of Privilege (2440591)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3963

Update Details

Recommendation is updated

10958 - (MS11-024) Microsoft Windows Fax Cover Page Editor Buffer Overflow Remote Code Execution (2527308)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4701

Update Details

Recommendation is updated

10977 - (MS10-104) Microsoft Windows SharePoint Could Allow Remote Code Execution (2455005)

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2010-3964

Update Details

Recommendation is updated

11224 - (MS11-013) Microsoft Kerberos Unkeyed Checksum (2496930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0043

Update Details

Recommendation is updated

11226 - (MS11-013) Vulnerabilities in Microsoft Kerberos Could Allow Elevation Of Privilege (2496930)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0043, CVE-2011-0091

Update Details

Recommendation is updated

11237 - (MS11-011) Windows Kernel Integer Truncation (2393802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0045

Update Details

Recommendation is updated

11243 - (MS11-014) Microsoft Local Security Authority Subsystem Service Length Validation (2478960)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0039

Update Details

Recommendation is updated

11244 - (MS11-012) Microsoft Win32k Improper User Input Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0086

Update Details

Recommendation is updated

11245 - (MS11-012) Microsoft Win32k Insufficient User Input Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0087

Update Details

Recommendation is updated

11246 - (MS11-012) Microsoft Win32k Window Class Pointer Confusion (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0088

Update Details

Recommendation is updated

11247 - (MS11-012) Microsoft Win32k Window Class Improper Pointer Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0089

Update Details

Recommendation is updated

11248 - (MS11-012) Microsoft Win32k Memory Corruption (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0090

Update Details

Recommendation is updated

11253 - (MS11-011) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (2393802)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4398, CVE-2011-0045

Update Details

Recommendation is updated

11265 - (MS11-014) Vulnerability In Local Security Authority Subsystem Service Could Allow Local Elevation Of Privilege (2478960)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0039

Update Details

Recommendation is updated

11266 - (MS11-012) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2479628)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0086, CVE-2011-0087, CVE-2011-0088, CVE-2011-0089, CVE-2011-0090

Update Details

Recommendation is updated

11786 - (MS11-024) Microsoft Fax Cover Page Editor Memory Corruption (2527308)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3974

Update Details

Recommendation is updated

11791 - (MS11-034) Microsoft Win32k Use After Free I (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0662

Update Details

Recommendation is updated

11792 - (MS11-034) Microsoft Win32k Use After Free II (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0665

Update Details

Recommendation is updated

11793 - (MS11-034) Microsoft Win32k Use After Free III (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0666

Update Details

Recommendation is updated

11794 - (MS11-034) Microsoft Win32k Use After Free IV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0667

Update Details

Recommendation is updated

11795 - (MS11-034) Microsoft Win32k Use After Free V (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0670

Update Details

Recommendation is updated

11796 - (MS11-034) Microsoft Win32k Use After Free VI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0671

Update Details

Recommendation is updated

11797 - (MS11-034) Microsoft Win32k Use After Free VII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0672

Update Details

Recommendation is updated

11798 - (MS11-034) Microsoft Win32k Use After Free VIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0674

Update Details

Recommendation is updated

11799 - (MS11-034) Microsoft Win32k Use After Free IX (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1234

Update Details

Recommendation is updated

11800 - (MS11-034) Microsoft Win32k Use After Free X (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1235

Update Details

Recommendation is updated

11801 - (MS11-034) Microsoft Win32k Use After Free XI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1236

Update Details

Recommendation is updated

11802 - (MS11-034) Microsoft Win32k Use After Free XII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1237

Update Details

Recommendation is updated

11803 - (MS11-034) Microsoft Win32k Use After Free XIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1238

Update Details

Recommendation is updated

11804 - (MS11-034) Microsoft Win32k Use After Free XIV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1239

Update Details

Recommendation is updated

11805 - (MS11-034) Microsoft Win32k Use After Free XV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1240

Update Details

Recommendation is updated

11806 - (MS11-034) Microsoft Win32k Use After Free XVI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1241

Update Details

Recommendation is updated

11807 - (MS11-034) Microsoft Win32k Use After Free XVII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1242

Update Details

Recommendation is updated

11808 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation I (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0673

Update Details

Recommendation is updated

11809 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation II (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0676

Update Details

Recommendation is updated

11810 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation III (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0677

Update Details

Recommendation is updated

11811 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation IV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1225

Update Details

Recommendation is updated

11812 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation V (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1226

Update Details

Recommendation is updated

11813 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1227

Update Details

Recommendation is updated

11814 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1228

Update Details

Recommendation is updated

11815 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1229

Update Details

Recommendation is updated

11816 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation IX (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1230

Update Details

Recommendation is updated

11817 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation X (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1231

Update Details

Recommendation is updated

11818 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation XI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1232

Update Details

Recommendation is updated

11819 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation XII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1233

Update Details

Recommendation is updated

11824 - (MS11-030) Microsoft DNS Crafted LLMNR Query Remote Code Execution (2509553)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0657

Update Details

Recommendation is updated

11836 - (MS11-034) Microsoft Win32k Use After Free XVIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0675

Update Details

Recommendation is updated

12221 - (MS11-046) Microsoft Windows Ancillary Function Driver Could Allow Elevation Of Privilege (2503665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1249

Update Details

Recommendation is updated

12222 - (MS11-042) Microsoft Windows DFS Referral Response Denial Of Service (KB2535512)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1869

Update Details

Recommendation is updated

12230 - (MS11-048) Microsoft Windows SMB Server Could Allow Denial Of Service (KB2536275)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1267

Update Details

Recommendation is updated

12248 - (MS11-046) Microsoft Windows Ancillary Function Driver Could Allow Elevation Of Privilege (2503665)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1249

Update Details

Recommendation is updated

12324 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation I (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1874

Update Details

Recommendation is updated

12325 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation II (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1875

Update Details

Recommendation is updated

12326 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation III (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1876

Update Details

Recommendation is updated

12327 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation IV (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1877

Update Details

Recommendation is updated

12328 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation V (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1878

Update Details

Recommendation is updated

12329 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VI (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1879

Update Details

Recommendation is updated

12330 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation I (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1880

Update Details

Recommendation is updated

12331 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation II (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1881

Update Details

Recommendation is updated

12332 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VII (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1882

Update Details

Recommendation is updated

12333 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VIII (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1883

Update Details

Recommendation is updated

12334 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation IX (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1884

Update Details

Recommendation is updated

12335 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation III (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1885

Update Details

Recommendation is updated

12337 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation IV (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1887

Update Details

Recommendation is updated

12338 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation V (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1888

Update Details

Recommendation is updated

12341 - (MS11-056) Microsoft Windows CSRSS Local EOP AllocConsole Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1281

Update Details

Recommendation is updated

12342 - (MS11-054) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1874, CVE-2011-1875, CVE-2011-1876, CVE-2011-1877, CVE-2011-1878, CVE-2011-1879, CVE-2011-1880, CVE-2011-1881, CVE-2011-1882, CVE-2011-1883, CVE-2011-1884, CVE-2011-1885, CVE-2011-1886, CVE-2011-1887, CVE-2011-1888

Update Details

Recommendation is updated

12343 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvSetConsoleLocalEUDC Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1282

Update Details

Recommendation is updated

12344 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvSetConsoleNumberOfCommand Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1283

Update Details

Recommendation is updated

12345 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvWriteConsoleOutput Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1284

Update Details

Recommendation is updated

12346 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvWriteConsoleOutputString Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1870

Update Details

Recommendation is updated

12442 - (MS11-062) Microsoft NDISTAPI Driver Could Allow Elevation Of Privilege (2566454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1974

Update Details

Recommendation is updated

12443 - (MS11-062) Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1974

Update Details

Recommendation is updated

12444 - (MS11-063) Microsoft WCRSS Could Allow Elevation Of Privilege (2567680)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1967

Update Details

Recommendation is updated

12445 - (MS11-063) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1967

Update Details

Recommendation is updated

12451 - (MS11-057) Microsoft Internet Explorer Windows Open Race Condition (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1257

Update Details

Recommendation is updated

12452 - (MS11-064) Microsoft TCP/IP Stack ICMP Could Allow Denial of Service (2563894)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1871

Update Details

Recommendation is updated

12453 - (MS11-064) Microsoft TCP/IP Stack QOS Could Allow Denial of Service (2563894)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1965

Update Details

Recommendation is updated

12460 - (MS11-065) Microsoft RDP Could Allow Denial Of Service (2570222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1968

Update Details

Recommendation is updated

12623 - (MS11-070) Microsoft Windows WINS Local Elevation of Privilege (2571621)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1984

Update Details

Recommendation is updated

12738 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k Null Pointer De-reference (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1985

Update Details

Recommendation is updated

12741 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k Use After Free (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2011

Update Details

Recommendation is updated

12758 - (MS11-080) Microsoft Ancillary Function Driver Elevation of Privilege (2592799)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2005

Update Details

Recommendation is updated

12762 - (MS11-080) Vulnerability In Ancillary Function Driver Elevation of Privilege (2592799)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2005

Update Details

Recommendation is updated

12913 - (MS11-084) Microsoft Windows TrueType Font Parsing Denial of Service (2617657)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2004

Update Details

Recommendation is updated

12914 - (MS11-084) Vulnerability in Microsoft Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2004

Update Details

Recommendation is updated

12980 - (MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMB

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2004-0123

Update Details

Recommendation is updated

12988 - (MS02-045) Microsoft Windows SMB DoS Remote Non-Intrusive

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2002-0724

Update Details

Recommendation is updated

13055 - (MS11-097) Microsoft Windows CSRSS Local Privilege Elevation (2620712)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3408

Update Details

Recommendation is updated

13056 - (MS11-098) Microsoft Windows Kernel Exception Handler (2633171)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2018

Update Details

Recommendation is updated

13058 - (MS11-088) Microsoft Office Pinyin IME Privilege Escalation (2652016)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2010

Update Details

Recommendation is updated

13059 - (MS11-097) Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2620712)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3408

Update Details

Recommendation is updated

13060 - (MS11-098) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2018

Update Details

Recommendation is updated

13070 - (MS11-088) Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2652016)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2010

Update Details

Recommendation is updated

13158 - (MS11-100) Microsoft Windows .NET Hash Tables Denial of Service (2659883)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3414

Update Details

Recommendation is updated

13290 - (MS12-009) Microsoft Windows AfdPoll Elevation of Privilege (2645640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0148

Update Details

Recommendation is updated

13291 - (MS12-008) Microsoft Windows Keyboard Layout Use After Free (2660465)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0154

Update Details

Recommendation is updated

13293 - (MS12-009) Microsoft Windows Ancillary Function Driver Elevation of Privilege (2645640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0149

Update Details

Recommendation is updated

13294 - (MS12-009) Vulnerabilities In Ancillary Function Driver Could Allow Elevation Of Privilege (2645640)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0148, CVE-2012-0149

Update Details

Recommendation is updated

13396 - (MS12-018) Microsoft Windows PostMessage Function Elevation of Privilege (2641653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0157

Update Details

Recommendation is updated

13399 - (MS12-018) Vulnerability In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2641653)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0157

Update Details

Recommendation is updated

13515 - (MS12-023) Microsoft Internet Explorer Print Feature Remote Code Execution (2675157)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0168

Update Details

Recommendation is updated

13616 - (MS12-032) Microsoft Windows TCP/IP Double Free Privilege Escalation (2688338)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0179

Update Details

Recommendation is updated

13619 - (MS12-032) Vulnerability In TCP/IP Could Allow Elevation Of Privilege (2688338)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0174, CVE-2012-0179

Update Details

Recommendation is updated

13620 - (MS12-033) Microsoft Windows Plug And Play Configuration Manager Privilege Escalation (2690533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0178

Update Details

Recommendation is updated

13621 - (MS12-033) Vulnerability In Windows Partition Manager Could Allow Elevation Of Privilege (2690533)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0178

Update Details

Recommendation is updated

13626 - (MS12-034) Microsoft Windows Scrollbar Calculation Privilege Escalation (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1848

Update Details

Recommendation is updated

13627 - (MS12-034) Microsoft Windows Keyboard Layout Privilege Escalation (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0181

Update Details

Recommendation is updated

13628 - (MS12-034) Microsoft Windows And Messages Privilege Escalation (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0180

Update Details

Recommendation is updated

13751 - (MS12-041) Microsoft Windows Clipboard Format Atom Name Handling Privilege Escalation (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1866

Update Details

Recommendation is updated

13776 - (MS12-041) Microsoft Windows Font Resource Refcount Integer Overflow Privilege Escalation (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1867

Update Details

Recommendation is updated

13777 - (MS12-041) Microsoft Windows String Atom Class Name Handling Privilege Escalation I (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1864

Update Details

Recommendation is updated

13778 - (MS12-041) Microsoft Windows String Atom Class Name Handling Privilege Escalation II (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1865

Update Details

Recommendation is updated

13781 - (MS12-042) Microsoft Windows User Mode Scheduler Memory Corruption Privilege Escalation (2711167)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0217

Update Details

Recommendation is updated

13785 - (MS12-041) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1864, CVE-2012-1865, CVE-2012-1866, CVE-2012-1867, CVE-2012-1868

Update Details

Recommendation is updated

13859 - (MS12-047) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1890, CVE-2012-1893

Update Details

Recommendation is updated

13860 - (MS12-047) Microsoft Windows Keyboard Layout Privilege Escalation (2718523)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1890

Update Details

Recommendation is updated

13861 - (MS12-047) Microsoft Windows Win32k Incorrect Type Handling Privilege Escalation (2718523)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1893

Update Details

Recommendation is updated

14016 - (MS12-055) Microsoft Windows Win32K User After Free Privilege Escalation (2731847)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2527

Update Details

Recommendation is updated

14212 - (MS12-065) Vulnerability In Microsoft Works Could Allow Remote Code Execution (2754670)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14215 - (MS12-068) Microsoft Windows Integer Overflow Information Disclosure (2724197)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2529

Update Details

Recommendation is updated

14218 - (MS12-068) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2529

Update Details

Recommendation is updated

14375 - (MS12-075) Microsoft Windows Win32k Use AfterFree Privilege Escalation I (2761226)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2530

Update Details

Recommendation is updated

14376 - (MS12-075) Microsoft Windows Win32k Use After Free Privilege Escalation II (2761159)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2553

Update Details

Recommendation is updated

14562 - (MS13-005) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0008

Update Details

Recommendation is updated

14563 - (MS13-005) Microsoft Windows Privilege Escalation (2778930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0008

Update Details

Recommendation is updated

14679 - (MS13-014) Microsoft Windows NFS NULL Dereference Denial Of Service (2790978)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1281

Update Details

Recommendation is updated

14688 - (MS13-018) Microsoft Windows TCP/IP FIN WAIT Denial Of Service (2790655)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0075

Update Details

Recommendation is updated

14690 - (MS13-019) Microsoft Windows CSRSS Reference Count Local Privilege Escalation (2790113)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0076

Update Details

Recommendation is updated

14711 - (MS13-012) Microsoft Exchange Server Oracle Outside In Denial Of Service I (2809279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0393

Update Details

Recommendation is updated

14712 - (MS13-012) Microsoft Exchange Server Oracle Outside In Denial Of Service II (2809279)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0418

Update Details

Recommendation is updated

14716 - (MS13-017) Microsoft Windows Race Condition I Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1278

Update Details

Recommendation is updated

14717 - (MS13-017) Microsoft Windows Race Condition II Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1279

Update Details

Recommendation is updated

14718 - (MS13-017) Microsoft Windows Reference Count Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1280

Update Details

Recommendation is updated

14735 - (MS13-012) Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2809279)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0393, CVE-2013-0418

Update Details

Recommendation is updated

14822 - (MS13-023) Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2801261)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0079

Update Details

Recommendation is updated

14827 - (MS13-023) Microsoft Visio Viewer Tree Object Type Confusion Remote Code Execution (2801261)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0079

Update Details

Recommendation is updated

14835 - (MS13-024) Microsoft SharePoint Server Buffer Overflow Denial of Service (2780176)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0085

Update Details

Recommendation is updated

14836 - (MS13-024) Microsoft SharePoint Server Callback Function Privilege Escalation (2780176)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0080

Update Details

Recommendation is updated

14837 - (MS13-024) Microsoft SharePoint Server Directory Traversal Privilege Escalation (2780176)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0084

Update Details

Recommendation is updated

14839 - (MS13-027) Microsoft Windows USB Descriptor Privilege Escalation I (2807986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1285

Update Details

Recommendation is updated

14840 - (MS13-027) Microsoft Windows USB Descriptor Privilege Escalation II (2807986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1286

Update Details

Recommendation is updated

14841 - (MS13-027) Microsoft Windows USB Descriptor Privilege Escalation III (2807986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1287

Update Details

Recommendation is updated

14844 - (MS13-027) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1285, CVE-2013-1286, CVE-2013-1287

Update Details

Recommendation is updated

14930 - (MS13-036) Microsoft Windows Kernel OpenType Font Parsing Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1291

Update Details

Recommendation is updated

14934 - (MS13-033) Vulnerability In Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2820917)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1295

Update Details

Recommendation is updated

14937 - (MS13-033) Microsoft Windows CSRSS Privilege Escalation (2820917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1295

Update Details

Recommendation is updated

14942 - (MS13-034) Microsoft Defender Antimalware Client Privilege Escalation (2823482)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0078

Update Details

Recommendation is updated

14943 - (MS13-034) Vulnerability in Microsoft Antimalware Client Could Allow Elevation of Privilege (2823482)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0078

Update Details

Recommendation is updated

15054 - (MS13-040) Vulnerabilities In .NET Framework Could Allow Spoofing (2836440)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1336, CVE-2013-1337

Update Details

Recommendation is updated

15069 - (MS13-046) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2840221)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1332, CVE-2013-1333, CVE-2013-1334

Update Details

Recommendation is updated

15070 - (MS13-046) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2840221)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1332

Update Details

Recommendation is updated

15071 - (MS13-046) Microsoft Windows Win32k Buffer Overflow Privilege Escalation (2840221)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1333

Update Details

Recommendation is updated

15072 - (MS13-046) Microsoft Windows Win32k Window Handle Privilege Escalation (2840221)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1334

Update Details

Recommendation is updated

15161 - (MS13-049) Microsoft Windows TCP/IP Driver Denial of Service (2845690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3138

Update Details

Recommendation is updated

15253 - (MS13-058) Vulnerability in Windows Defender Could Allow Elevation of Privilege (2847927)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3154

Update Details

Recommendation is updated

15254 - (MS13-058) Microsoft Windows Defender Improper PathName Privilege Escalation (2847927)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3154

Update Details

Recommendation is updated

15281 - (MS13-053) Microsoft Windows Kernel Read AV Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3660

Update Details

Recommendation is updated

15360 - (MS13-065) Vulnerability in ICMPv6 could allow Denial of Service (2868623)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3183

Update Details

Recommendation is updated

15365 - (MS13-063) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (2859537)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-2556, CVE-2013-3196, CVE-2013-3197, CVE-2013-3198

Update Details

Recommendation is updated

15576 - (MS13-076) Vulnerabilities In Kernel-Mode Drivers Could Allow Elevation Of Privilege (2876315)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1341, CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, CVE-2013-3865, CVE-2013-3866

Update Details

Recommendation is updated

15933 - (MS13-093) Microsoft Windows Ancillary Function Driver Information Disclosure (2875783)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3887

Update Details

Recommendation is updated

15934 - (MS13-093) Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3887

Update Details

Recommendation is updated

16014 - (MS13-096) Microsoft Graphics Component Memory Corruption Remote Code Execution (2908005)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3906

Update Details

Recommendation is updated

16023 - (MS13-097) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5047

Update Details

Recommendation is updated

16024 - (MS13-101) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3899, CVE-2013-3902, CVE-2013-3903, CVE-2013-3907, CVE-2013-5058

Update Details

Recommendation is updated

16207 - (MS14-003) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2913602)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0262

Update Details

Recommendation is updated

16313 - (MS14-006) Vulnerability in TCP/IP IPv6 Could Allow Denial of Service (2904659)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

16327 - (MS14-005) Vulnerability In Microsoft XML Core Services Could Allow Information Disclosure (2916036)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0266

Update Details

Recommendation is updated

16397 - (MS14-014) Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0319

Update Details

Recommendation is updated

16398 - (MS14-014) Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-0319

Update Details

Recommendation is updated

16399 - (MS14-014) Microsoft Silverlight DEP/ASLR Security Bypass (2932677)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0319

Update Details

Recommendation is updated

16400 - (MS14-015) Vulnerabilities in Windows Kernel Mode Driver Could Allow Elevation of Privilege (2930275)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0300, CVE-2014-0323

Update Details

Recommendation is updated

16401 - (MS14-015) Microsoft Windows Kernel Mode Driver Win32k Privilege Escalation Privilege (2930275)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0300

Update Details

Recommendation is updated

16600 - (MS14-023) Vulnerability in Microsoft Office Could Allow Remote Code Execution (2961037)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1756, CVE-2014-1808

Update Details

Recommendation is updated

16705 - (MS14-031) Vulnerability in TCP Protocol Could Allow Denial of Service (2962478)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1811

Update Details

Recommendation is updated

16873 - (MS14-042) Microsoft Windows Service Bus Denial of Service (2972621)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2814

Update Details

Recommendation is updated

17011 - (MS14-045) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2984615)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0318, CVE-2014-1819, CVE-2014-4064

Update Details

Recommendation is updated

17227 - (MS14-058) Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4113, CVE-2014-4148

Update Details

Recommendation is updated

17262 - (MS14-063) Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (2998579)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4115

Update Details

Recommendation is updated

33093 - Oracle Solaris 148071-15 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-0166, CVE-2013-0169, CVE-2014-0224, CVE-2014-3508, CVE-2014-3511, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated Risk is updated CVE is updated FASLScript is updated

58243 - Debian Linux 6.0 DSA-2344-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2011-4103

Update Details

Risk is updated

58350 - Debian Linux 6.0 DSA-2442-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2010-5077

Update Details

Risk is updated

58353 - Debian Linux 6.0 DSA-2442-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2010-5077

Update Details

Risk is updated

86451 - Fedora Linux 17 FEDORA-2012-5371 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2010-5077

Update Details

Risk is updated

87270 - Fedora Linux 18 FEDORA-2012-19879 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2012-5580

Update Details

Risk is updated

1111 - (MS02-045) Microsoft Windows SMB Denial-of-Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0724

Update Details

Recommendation is updated

2052 - (MS03-022) Microsoft Windows Media Services ISAPI Extension Command Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0349, CVE-2003-0227

Update Details

Recommendation is updated

2086 - (MS03-051) Microsoft FPSE SmartHTML Interpreter Denial-of-Service

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2003-0822, CVE-2003-0824

Update Details

Recommendation is updated

2110 - (MS03-027) Microsoft Windows Shell EXPLORER.EXE Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0306, CVE-2003-0351

Update Details

Recommendation is updated

2445 - (MS03-021) Microsoft Windows Media Player Library Access

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0348

Update Details

Recommendation is updated

2983 - (MS04-044) Microsoft Windows Kernel Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-0893, CVE-2004-0894

Update Details

Recommendation is updated

3296 - (MS02-053) Microsoft Windows SmartHTML Interpreter Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0692

Update Details

Recommendation is updated

3402 - (MS05-024) Microsoft Windows Explorer (Web View) Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1191

Update Details

Recommendation is updated

3403 - (MS05-021) Microsoft Exchange Remote Code Execution

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Medium

CVE: CVE-2005-0560

Update Details

Recommendation is updated

3407 - (MS05-031) Microsoft Windows Interactive Training Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1212

Update Details

Recommendation is updated

3410 - (MS05-030) Microsoft Outlook Express NNTP Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1213

Update Details

Recommendation is updated

3646 - (MS05-046) Microsoft Windows Netware Client Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1985

Update Details

Recommendation is updated

3896 - (MS05-047) Microsoft Windows Plug And Play Service Arbitrary Code Execution Vulnerability (905749)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2120

Update Details

Recommendation is updated

3988 - (MS05-054) Microsoft Internet Explorer Mismatched Document Object

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1790, CVE-2005-2829, CVE-2005-2830, CVE-2005-2831, CVE-2006-0057

Update Details

Recommendation is updated

3990 - (MS05-055) Microsoft Windows Kernel Privilege Escalation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2827

Update Details

Recommendation is updated

4092 - (MS06-008) Microsoft Windows Web Client Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0013

Update Details

Recommendation is updated

4095 - (MS06-007) Microsoft Windows TCP/IP Stack Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0021

Update Details

Recommendation is updated

4362 - (MS06-016) Microsoft Outlook Express Windows Address Book Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0014

Update Details

Recommendation is updated

4499 - (MS06-044) Microsoft Management Console Redirect Cross-Site Scripting Vulnerability (KB917008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-3643

Update Details

Recommendation is updated

4663 - (MS06-067) Microsoft DirectAnimation ActiveX Controls Memory Corruption Vulnerability II (922760)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-4446, CVE-2006-4687, CVE-2006-4777, CVE-2006-5884

Update Details

Recommendation is updated

4707 - (MS05-054) Microsoft Internet Explorer Download Dialog Box Manipulation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1790, CVE-2005-2829, CVE-2005-2830, CVE-2005-2831, CVE-2006-0057

Update Details

Recommendation is updated

4708 - (MS05-054) Microsoft Internet Explorer HTTPS Proxy

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1790, CVE-2005-2829, CVE-2005-2830, CVE-2005-2831, CVE-2006-0057

Update Details

Recommendation is updated

5227 - (MS07-032) Microsoft Permissive User Information Store ACLs Information Disclosure Vulnerability (931213) (931213)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-2229

Update Details

Recommendation is updated

5324 - (MS07-038) Microsoft Vista Firewall Blocking Rule Information Disclosure Vulnerability (935807)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3038

Update Details

Recommendation is updated

5419 - (MS07-047) Microsoft Windows Media Player Code Execution Vulnerability Decompressing Skins (936782)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3035, CVE-2007-3037

Update Details

Recommendation is updated

5420 - (MS07-047) Microsoft Windows Media Player Code Execution Vulnerability Parsing Skins (936782)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3035, CVE-2007-3037

Update Details

Recommendation is updated

5424 - (MS07-048) Microsoft Vista Feed Headlines Gadget Remote Code Execution Vulnerability (938123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3033, CVE-2007-3032, CVE-2007-3891

Update Details

Recommendation is updated

5478 - (MS07-053) Microsoft Windows Services for UNIX Could Allow Elevation of Privilege (939778)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3036

Update Details

Recommendation is updated

5479 - (MS07-052) Microsoft Crystal Reports RPT Processing Vulnerability (941522)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-6133

Update Details

Recommendation is updated

5654 - (MS08-002) Microsoft LSASS Bypass Vulnerability (943485)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-5352

Update Details

Recommendation is updated

5925 - (MS08-034) Microsoft Memory Overwrite Vulnerability (948745)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-1451

Update Details

Recommendation is updated

5990 - (MS08-039) Microsoft Outlook Web Access for Exchange Server Parsing Cross-Site Scripting Vulnerability (953747)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2247, CVE-2008-2248

Update Details

Recommendation is updated

5996 - (MS08-041) Microsoft Snapshot Viewer Arbitrary File Download and Install Vulnerability (955617)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2463

Update Details

Recommendation is updated

6136 - (MS09-001) SMB Validation Denial of Service Vulnerability (958687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4114

Update Details

Recommendation is updated

6161 - (MS08-066) Microsoft AFD Kernel Overwrite Vulnerability (956803)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-3464

Update Details

Recommendation is updated

6164 - (MS08-064) Microsoft Virtual Address Descriptor Elevation of Privilege Vulnerability (956841)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4036

Update Details

Recommendation is updated

6169 - (MS08-061) Microsoft Windows Kernel Window Creation Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2250

Update Details

Recommendation is updated

6170 - (MS08-061) Microsoft Windows Kernel Unhandled Exception Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2251

Update Details

Recommendation is updated

6171 - (MS08-061) Microsoft Windows Kernel Memory Corruption Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2252

Update Details

Recommendation is updated

6423 - (MS09-003) Microsoft Exchange Literal Processing Vulnerability (959239)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0099

Update Details

Recommendation is updated

6493 - (MS09-006) Windows Kernel Handle Validation Vulnerability (958690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0082

Update Details

Recommendation is updated

6494 - (MS09-006) Windows Kernel Invalid Pointer Vulnerability (958690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0083

Update Details

Recommendation is updated

6600 - (MS09-012) Microsoft Windows RPCSS Service Isolation Vulnerability (959454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0079

Update Details

Recommendation is updated

6601 - (MS09-012) Microsoft Windows Thread Pool ACL Weakness Vulnerability (959454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0080

Update Details

Recommendation is updated

6602 - (MS09-012) Microsoft Windows WMI Service Isolation Vulnerability (959454)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0078

Update Details

Recommendation is updated

6603 - (MS09-013) Microsoft Windows HTTP Services Certificate Name Mismatch Vulnerability (960803)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0089

Update Details

Recommendation is updated

6613 - (MS09-016) Microsoft ISA Server Web Proxy TCP State Limited Denial of Service (961759)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0077

Update Details

Recommendation is updated

6679 - Microsoft Internet Information Services WebDAV Security Bypass Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2009-1535, CVE-2009-1676

Update Details

Recommendation is updated

6744 - (MS09-019) Microsoft Internet Explorer Cross-Domain Information Disclosure Vulnerability (969897)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1140

Update Details

Recommendation is updated

6753 - (MS09-020) Microsoft IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability (970483)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1535, CVE-2009-1676

Update Details

Recommendation is updated

6766 - (MS09-025) Microsoft Windows Desktop Parameter Edit Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1126

Update Details

Recommendation is updated

6767 - (MS09-025) Microsoft Windows Driver Class Registration Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1125

Update Details

Recommendation is updated

6768 - (MS09-025) Microsoft Windows Kernel Desktop Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1123

Update Details

Recommendation is updated

6769 - (MS09-025) Microsoft Windows Kernel Pointer Validation Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1124

Update Details

Recommendation is updated

7107 - (MS09-048) Microsoft Windows TCP/IP Orphaned Connections Vulnerability (967723)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1926

Update Details

Recommendation is updated

7203 - (MS09-058) Windows Kernel Integer Underflow Vulnerability (971486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2515

Update Details

Recommendation is updated

7204 - (MS09-058) Windows Kernel NULL Pointer Dereference Vulnerability (971486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2516

Update Details

Recommendation is updated

7205 - (MS09-059) Local Security Authority Subsystem Service Integer Overflow Vulnerability (975467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2524

Update Details

Recommendation is updated

7228 - (MS09-056) Vulnerabilities In Windows CryptoAPI Could Allow Spoofing (974571)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2511, CVE-2009-2510

Update Details

Recommendation is updated

7231 - (MS09-059) Vulnerability In Local Security Authority Subsystem Service Could Allow Denial Of Service (975467)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2524

Update Details

Recommendation is updated

7342 - Microsoft Windows SMB_PACKET Remote Kernel Denial-of-Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3676

Update Details

Recommendation is updated

7415 - (MS09-008) Vulnerabilities In DNS and WINS Server Could Allow Spoofing (962238)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0093, CVE-2009-0094, CVE-2009-0233, CVE-2009-0234

Update Details

Recommendation is updated

7450 - (MS09-070) Single Sign On Spoofing in ADFS Vulnerability (971726)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2508

Update Details

Recommendation is updated

7454 - (MS09-069) Local Security Authority Subsystem Service Resource Exhaustion Vulnerability (974392)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3675

Update Details

Recommendation is updated

7464 - (MS09-069) Vulnerability In Local Security Authority Subsystem Service Could Allow Denial of Service (974392)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3675

Update Details

Recommendation is updated

7544 - (MS09-025) Vulnerabilities In Windows Kernel Could Allow Elevation of Privilege (968537)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1123, CVE-2009-1124, CVE-2009-1125, CVE-2009-1126

Update Details

Recommendation is updated

7625 - (MS08-002) Vulnerability In LSASS Could Allow Local Elevation Of Privilege (943485)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-5352

Update Details

Recommendation is updated

7723 - (MS10-002) Microsoft Internet Explorer XSS Filter Script Handling Vulnerability (978207)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-4074

Update Details

Recommendation is updated

7828 - (MS08-036) Vulnerabilities In Pragmatic General Multicast (PGM) Could Allow Denial Of Service (950762)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-1441, CVE-2008-1440

Update Details

Recommendation is updated

7852 - (MS10-014) Microsoft Windows Kerberos Null Pointer Dereference Vulnerability (977290)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0035

Update Details

Recommendation is updated

8054 - (MS08-064) Vulnerability In Virtual Address Descriptor Manipulation Could Allow Elevation Of Privilege (956841)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4036

Update Details

Recommendation is updated

8132 - (MS08-066) Vulnerability In The Microsoft Ancillary Function Driver Could Allow Elevation Of Privilege (956803)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-3464

Update Details

Recommendation is updated

8521 - (MS10-021) Microsoft Windows Kernel Memory Allocation Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0236

Update Details

Recommendation is updated

8522 - (MS10-021) Microsoft Windows Kernel Symbolic Link Creation Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0237

Update Details

Recommendation is updated

9073 - (MS10-032) Microsoft Windows Win32k Improper Data Validation Vulnerability (979559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0484

Update Details

Recommendation is updated

9074 - (MS10-032) Microsoft Windows Win32k Window Creation Vulnerability (979559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0485

Update Details

Recommendation is updated

9075 - (MS10-032) Microsoft Windows Win32k TrueType Font Parsing Vulnerability (979559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1255

Update Details

Recommendation is updated

9076 - (MS10-037) Microsoft Windows OpenType CFF Font Driver Memory Corruption Vulnerability (980218)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0819

Update Details

Recommendation is updated

9086 - (MS10-041) Microsoft Windows .NET Framework XML Signature HMAC Truncation Bypass Vulnerability (981343)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0217

Update Details

Recommendation is updated

9679 - (MS10-058) Microsoft Windows Integer Overflow in Windows Networking Privilege Escalation (978886)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1893

Update Details

Recommendation is updated

9682 - (MS10-047) Microsoft Windows Kernel Improper Validation Denial Of Service (981852)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1890

Update Details

Recommendation is updated

9683 - (MS10-047) Microsoft Windows Kernel Double Free Privilege Escalation (981852)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1889

Update Details

Recommendation is updated

9684 - (MS10-047) Microsoft Windows Kernel Data Initialization Privilege Escalation (981852)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1888

Update Details

Recommendation is updated

9690 - (MS10-059) Microsoft Windows Tracing Memory Corruption Privilege Escalation (982799)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2555

Update Details

Recommendation is updated

9691 - (MS10-059) Microsoft Windows Tracing Registry Key ACL Privilege Escalation (982799)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2554

Update Details

Recommendation is updated

10037 - (MS10-069) Microsoft Windows CSRSS Local Elevation of Privilege (2121546)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1891

Update Details

Recommendation is updated

10040 - (MS10-065) Microsoft IIS Directory Authentication Bypass Privilege Escalation (2267960)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2731

Update Details

Recommendation is updated

10104 - (MS10-070) Microsoft ASP.NET AES Decrypt Security Bypass (2416728)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3332

Update Details

Recommendation is updated

10168 - (MS10-070) Microsoft ASP.NET AES Decrypt Security Bypass (2416728)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2010-3332

Update Details

Recommendation is updated

10321 - (MS10-084) Microsoft Windows LPC Message Buffer Overrun Privilege Escalation (2360937)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3222

Update Details

Recommendation is updated

10328 - (MS10-072) Microsoft Sharepoint HTML Sanitization Information Disclosure (2412048) I

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3243

Update Details

Recommendation is updated

10329 - (MS10-072) Microsoft SharePoint HTML Sanitization Information Disclosure (2412048) II

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3324

Update Details

Recommendation is updated

10358 - (MS10-073) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2549, CVE-2010-2743, CVE-2010-2744

Update Details

Recommendation is updated

10360 - (MS10-073) Microsoft Windows Win32K Reference Count Privilege Escalation (981957)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2549

Update Details

Recommendation is updated

10361 - (MS10-073) Microsoft Windows Win32K Keyboard Layout Privilege Escalation (981957)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2743

Update Details

Recommendation is updated

10362 - (MS10-073) Microsoft Windows Win32k Window Class Privilege Escalation (981957)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2744

Update Details

Recommendation is updated

10363 - (MS10-081) Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2746

Update Details

Recommendation is updated

11429 - (MS02-053) Microsoft Windows SmartHTML Interpreter Buffer Overflow

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2002-0692

Update Details

Recommendation is updated

13125 - (MS05-047) Microsoft Windows Plug And Play Service Arbitrary Code Execution Vulnerability (905749)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Medium

CVE: CVE-2005-2120

Update Details

Recommendation is updated

15362 - (MS13-061) Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2876063)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-2393, CVE-2013-3776, CVE-2013-3781

Update Details

Recommendation is updated

16046 - (MS13-100) Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (2904244)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5059

Update Details

Recommendation is updated

16402 - (MS14-015) Microsoft Windows Kernel Mode Driver Win32k Information Disclosure (2930275)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0323

Update Details

Recommendation is updated

16496 - (MS14-019) Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2922229)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0315

Update Details

Recommendation is updated

16593 - (MS14-025) Microsoft Active Directory Group Policy Preferences Password Privilege Escalation (2962486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1812

Update Details

Recommendation is updated

16595 - (MS14-025) Vulnerability in Active Directory Could Allow Elevation of Privilege (2962486)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1812

Update Details

Recommendation is updated

16841 - (MS14-041) Vulnerability in DirectShow Could Allow Elevation of Privilege (2975681)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2780

Update Details

Recommendation is updated

16961 - (MS14-044) Vulnerabilities in SQL Server Could Allow Elevation of Privilege (2984340)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1820, CVE-2014-4061

Update Details

Recommendation is updated

58851 - Debian Linux 7.0 DSA-2948-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3137

Update Details

Risk is updated

142378 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1039-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3564

Update Details

Risk is updated

181239 - FreeBSD gpgme Heap-based Buffer Overflow In Gpgsm Status Handler (90ca3ba5-19e6-11e4-8616-001b3856973b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3564

Update Details

Risk is updated

184509 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2307-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3564

Update Details

Risk is updated

188158 - Fedora Linux 20 FEDORA-2014-8334 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3137

Update Details

Risk is updated

188169 - Fedora Linux 19 FEDORA-2014-8328 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3137

Update Details

Risk is updated

188205 - Fedora Linux 20 FEDORA-2014-9694 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-5075

Update Details

Risk is updated

188251 - Fedora Linux 21 FEDORA-2014-10691 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3604

Update Details

Risk is updated

188286 - Fedora Linux 19 FEDORA-2014-10746 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3604

Update Details

Risk is updated

188297 - Fedora Linux 20 FEDORA-2014-10729 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3604

Update Details

Risk is updated

1845 - (MS03-018) Microsoft Windows IIS Cumulative Patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0225

Update Details

Recommendation is updated

1861 - (MS03-013) Microsoft Windows Kernel Message Handling Buffer Overflow

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0112

Update Details

Recommendation is updated

2102 - (MS04-030) Microsoft IIS WebDAV XML Handler Denial-of-Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0718, CVE-2004-0270

Update Details

Recommendation is updated

2189 - (MS04-012) Microsoft Windows RPC DCOM Cumulative Update

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0807, CVE-2003-0813, CVE-2004-0116, CVE-2004-0124

Update Details

Recommendation is updated

2272 - (MS04-012) Microsoft Windows RPC DCOM REMOTE Cumulative Update

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Medium

CVE: CVE-2003-0807, CVE-2003-0813, CVE-2004-0116, CVE-2004-0124

Update Details

Recommendation is updated

2281 - (MS04-011) Microsoft Windows SSL Library Denial-of-Service

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2004-0120

Update Details

Recommendation is updated

2416 - (MS04-016) Microsoft Windows DirectPlay Denial-of-Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-0202

Update Details

Recommendation is updated

2500 - (MS02-060) Flaw in Windows XP Help and Support Center Could Enable File Deletion

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0974

Update Details

Recommendation is updated

2501 - (MS02-070) Flaw in SMB Signing Could Enable Group Policy to be Modified

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-1256

Update Details

Recommendation is updated

2563 - (MS04-018) Microsoft Outlook Express Denial-of-Service Patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-0215

Update Details

Recommendation is updated

2645 - (MS02-071) Microsoft Windows WM_TIMER Message Flaw Privilege Escalation

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-1230

Update Details

Recommendation is updated

3027 - (MS05-001) Microsoft Windows HTML Help ActiveX Control Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-1043

Update Details

Recommendation is updated

3134 - (MS05-013) Microsoft Windows DHTML Editing ActiveX Control Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-1319

Update Details

Recommendation is updated

3194 - (MS05-006) Microsoft SharePoint Cross-Site Scripting and Spoofing

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2005-0049

Update Details

Recommendation is updated

3195 - (MS05-006) Microsoft SharePoint Cross-Site Scripting and Spoofing Patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-0049

Update Details

Recommendation is updated

3300 - (MS02-008) Microsoft XMLHTTP Control Unauthorized File Access

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0057

Update Details

Recommendation is updated

3301 - (MS02-048) Microsoft Certificate Enrollment Control Unauthorized Certificate Deletion

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0699

Update Details

Recommendation is updated

3405 - (MS05-025) Microsoft Internet Explorer XML Redirect Information Disclosure

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0648, CVE-2005-1211

Update Details

Recommendation is updated

3414 - (MS05-032) Microsoft MSAgent ActiveX Spoofing

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1214

Update Details

Recommendation is updated

3416 - (MS05-033) Microsoft Windows Telnet Information Disclosure

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1205

Update Details

Recommendation is updated

3613 - (MS05-037) Microsoft Internet Explorer JView Profiler Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2087

Update Details

Recommendation is updated

3644 - (MS05-042) Microsoft Windows Kerberos Multiple Issues

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1981, CVE-2005-1982

Update Details

Recommendation is updated

3647 - (MS05-041) Microsoft Windows Terminal Service RDP Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-1218, CVE-2005-2303

Update Details

Recommendation is updated

3890 - (MS05-050) Microsoft DirectShow Remote Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2128

Update Details

Recommendation is updated

4184 - (MS06-011) Microsoft Windows Permissive Windows Services DACL

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0023

Update Details

Recommendation is updated

4378 - (MS06-020) Macromedia Flash Player Frame Type Identifier Handling Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2628, CVE-2006-0024

Update Details

Recommendation is updated

4379 - (MS06-020) Macromedia Flash Player Invalid Memory Access

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0024, CVE-2005-2628

Update Details

Recommendation is updated

4443 - (MS06-033) Microsoft ASP.NET Application Folder Information Disclosure Vulnerability (917283)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-1300

Update Details

Recommendation is updated

4444 - (MS06-034) Internet Information Services using Malformed Active Server Pages Vulnerability (917537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0026

Update Details

Recommendation is updated

4505 - (MS06-047) Microsoft Visual Basic for Applications Vulnerability (KB921645)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-3649

Update Details

Recommendation is updated

4511 - (MS06-045) Microsoft Windows Explorer Folder GUID Code Execution Vulnerability (KB921398)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-3281

Update Details

Recommendation is updated

4602 - (MS06-053) Microsoft Windows Indexing Service Vulnerability (920685)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-0032, CVE-2006-5152

Update Details

Recommendation is updated

4679 - (MS06-064) Microsoft ICMP Connection Reset Vulnerability (922819)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-0790, CVE-2004-0230, CVE-2005-0688

Update Details

Recommendation is updated

4681 - (MS06-064) Microsoft TCP Connection Reset Vulnerability (922819)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2004-0790, CVE-2005-0688

Update Details

Recommendation is updated

4682 - (MS06-064) Microsoft Spoofed Connection Request Vulnerability (922819)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-0688, CVE-2004-0230, CVE-2004-0790

Update Details

Recommendation is updated

4697 - (MS05-025) Microsoft Internet Explorer PNG Rendering Memory Corruption

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0648, CVE-2005-1211

Update Details

Recommendation is updated

4815 - (MS07-021) Microsoft MsgBox (CSRSS) Remote Code Execution Vulnerability (930178)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-6696

Update Details

Recommendation is updated

5016 - (MS07-033) Microsoft Internet Explorer 7 Navigation Cancel Page Spoofing Vulnerability (933566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-1499, CVE-2007-1752

Update Details

Recommendation is updated

5425 - (MS07-048) Microsoft Vista Contacts Gadget Remote Code Execution Vulnerability (938123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3032, CVE-2007-3033, CVE-2007-3891

Update Details

Recommendation is updated

5430 - (MS07-048) Microsoft Vista Weather Gadget Remote Code Execution Vulnerability (938123)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-3891, CVE-2007-3032, CVE-2007-3033

Update Details

Recommendation is updated

5497 - (MS07-059) Microsoft SharePoint Scripting Vulnerability (942017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-2581

Update Details

Recommendation is updated

5550 - (MS07-067) Microsoft Windows Macrovision Driver Vulnerability (944653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-5587

Update Details

Recommendation is updated

5695 - (MS08-003) Microsoft Active Directory Vulnerability (946538)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-0088

Update Details

Recommendation is updated

5989 - (MS08-039) Microsoft Outlook Web Access for Exchange Server Data Validation Cross-Site Scripting Vulnerability (953747)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2247 , CVE-2008-2248

Update Details

Recommendation is updated

6166 - (MS08-056) Microsoft Content-Disposition Header Vulnerability (957699)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4020

Update Details

Recommendation is updated

6496 - (MS09-008) Microsoft DNS Server Query Validation Vulnerability (962238)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0233

Update Details

Recommendation is updated

6497 - (MS09-008) Microsoft DNS Server Response Validation Vulnerability (962238)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0234

Update Details

Recommendation is updated

6498 - (MS09-008) Microsoft DNS Server Vulnerability in WPAD Registration Vulnerability (962238)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0093

Update Details

Recommendation is updated

6499 - (MS09-008) Microsoft WPAD WINS Server Registration Vulnerability (962238)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0094

Update Details

Recommendation is updated

6612 - (MS09-016) Microsoft ISA Server Cross Site Scripting Vulnerability (961759)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0237

Update Details

Recommendation is updated

6763 - (MS09-022) Microsoft Windows Print Spooler Read File Vulnerability (961501)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0229

Update Details

Recommendation is updated

6764 - (MS09-023) Microsoft Windows Script Execution in Windows Search Vulnerability (963093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0239

Update Details

Recommendation is updated

6965 - (MS09-040) Microsoft MSMQ Null Pointer Vulnerability (971032)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1922

Update Details

Recommendation is updated

7200 - (MS09-056) Null Truncation in X.509 Common Name Vulnerability (974571)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2510

Update Details

Recommendation is updated

7202 - (MS09-058) Windows Kernel Exception Handler Vulnerability (971486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2517

Update Details

Recommendation is updated

7354 - (MS09-016) Vulnerabilities In Microsoft ISA Server And Forefront Threat Management Gateway Could Cause Denial Of Service (961759

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0077, CVE-2009-0237

Update Details

Recommendation is updated

7405 - Microsoft Internet Explorer 'DC:TITLE' PDF Information Disclosure Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-4073

Update Details

Risk is updated

7424 - (MS09-040) Vulnerability In Message Queuing Could Allow Elevation Of Privilege (971032)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1922

Update Details

Recommendation is updated

7542 - (MS09-023) Vulnerability In Windows Search Could Allow Information Disclosure (963093)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0239

Update Details

Recommendation is updated

7812 - (MS08-056) Vulnerability In Microsoft Office Could Allow Information Disclosure (957699)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4020

Update Details

Recommendation is updated

7853 - (MS10-010) Microsoft Windows Hyper-V Instruction Set Validation Vulnerability (977894)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0026

Update Details

Recommendation is updated

7855 - (MS10-011) Microsoft Windows CSRSS Local Privilege Escalation Vulnerability (978037)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0023

Update Details

Recommendation is updated

7884 - (MS10-010) Vulnerability In Windows Server 2008 Hyper-V Could Allow Denial Of Service (977894)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0026

Update Details

Recommendation is updated

7885 - (MS10-011) Vulnerability In Windows Client/Server Run-time Subsystem Could Allow Elevation Of Privilege (978037)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0023

Update Details

Recommendation is updated

7888 - (MS10-014) Vulnerability In Kerberos Could Allow Denial Of Service (977290)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0035

Update Details

Recommendation is updated

8517 - (MS10-029) Microsoft Windows ISATAP IPv6 Source Address Spoofing Vulnerability (978338)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0812

Update Details

Recommendation is updated

8519 - (MS10-021) Microsoft Windows Kernel Null Pointer Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0234

Update Details

Recommendation is updated

8520 - (MS10-021) Microsoft Windows Kernel Symbolic Link Value Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0235

Update Details

Recommendation is updated

8523 - (MS10-021) Microsoft Windows Kernel Registry Key Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0238

Update Details

Recommendation is updated

8524 - (MS10-021) Microsoft Windows Virtual Path Parsing Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0481

Update Details

Recommendation is updated

8525 - (MS10-021) Microsoft Windows Kernel Malformed Image Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0482

Update Details

Recommendation is updated

8526 - (MS10-021) Microsoft Windows Kernel Exception Handler Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0810

Update Details

Recommendation is updated

8538 - (MS10-024) Microsoft SMTP Server MX Record Vulnerability (981832)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0024

Update Details

Recommendation is updated

8539 - (MS10-024) Microsoft SMTP Memory Allocation Vulnerability (981832)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0025

Update Details

Recommendation is updated

8548 - (MS10-024) Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0024, CVE-2010-0025

Update Details

Recommendation is updated

9063 - (MS10-032) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (979559)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0484, CVE-2010-0485, CVE-2010-1255

Update Details

Recommendation is updated

9067 - (MS10-039) Vulnerabilities In Microsoft SharePoint Could Allow Elevation Of Privilege (2028554)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0817, CVE-2010-1257, CVE-2010-1264

Update Details

Recommendation is updated

9069 - (MS10-041) Vulnerabilities In The Microsoft .NET Framework Could Allow Tampering (981343)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0217

Update Details

Recommendation is updated

9077 - (MS10-035) Microsoft Internet Explorer toStaticHTML Information Disclosure Vulnerability (982381)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1257

Update Details

Recommendation is updated

9119 - (MS10-039) Microsoft SharePoint toStaticHTML Information Disclosure Vulnerability (2028554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1257

Update Details

Recommendation is updated

9381 - (MS11-050) Microsoft Internet Explorer 'mshtml.dll' Remote Information Disclosure Vulnerability (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3886

Update Details

Recommendation is updated

9719 - (MS10-059) Vulnerabilities in the Tracing Feature for Services Could Allow an Elevation of Privilege (982799)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2554, CVE-2010-2555

Update Details

Recommendation is updated

9763 - (MS10-049) Microsoft Windows TLS/SSL Renegotiation Vulnerability (980436)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3555

Update Details

Recommendation is updated

10048 - (MS10-069) Vulnerability In Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2121546)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1891

Update Details

Recommendation is updated

10199 - (MS10-070) Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3332

Update Details

Recommendation is updated

10312 - (MS10-072) Vulnerabilities in SafeHTML Could Allow Information Disclosure (2412048)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3243, CVE-2010-3324

Update Details

Recommendation is updated

10558 - Microsoft Windows Environment Variable Expansion Library Loading Vulnerability (329308)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-6753

Update Details

Recommendation is updated

10867 - (MS10-102) Vulnerability in Hyper-V Could Allow Denial of Service (2345316)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3960

Update Details

Recommendation is updated

10870 - (MS10-101) Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2742

Update Details

Recommendation is updated

10878 - (MS10-101) Microsoft Windows Netlogon Service Could Allow Denial Of Service (2207559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2742

Update Details

Recommendation is updated

10887 - (MS10-102) Microsoft Windows Hyper-V Could Allow Denial of Service (2345316)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3960

Update Details

Recommendation is updated

10891 - (MS10-090) Microsoft Internet Explorer Cross-Domain Information Disclosure Vulnerability CVE-2010-3342 (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3342

Update Details

Recommendation is updated

10895 - (MS10-090) Microsoft Internet Explorer Cross-Domain Information Disclosure Vulnerability CVE-2010-3348 (2416400)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3348

Update Details

Recommendation is updated

11175 - (MS11-026) Microsoft MHTML Mime-Formatted Request (2503658)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0096

Update Details

Recommendation is updated

11225 - (MS11-013) Microsoft Kerberos Spoofing (2496930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0091

Update Details

Recommendation is updated

11240 - (MS11-009) Microsoft Scripting Engines Information Disclosure (2475792)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0031

Update Details

Recommendation is updated

11241 - (MS11-010) Windows Client/Server Run-time Subsystem Elevation of Privilege (2476687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0030

Update Details

Recommendation is updated

11242 - (MS11-005) Microsoft Active Directory SPN Validation (2478953)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0040

Update Details

Recommendation is updated

11255 - (MS11-009) Vulnerability In JScript And VBScript Scripting Engines Could Allow Information Disclosure (2475792)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0031

Update Details

Recommendation is updated

11256 - (MS11-010) Vulnerability In Windows Client/Server Run-time Subsystem Could Allow Elevation Of Privilege (2476687)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0030

Update Details

Recommendation is updated

11257 - (MS11-005) Vulnerability In Active Directory Could Allow Denial of Service (2478953)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0040

Update Details

Recommendation is updated

11762 - (MS11-026) Vulnerability in MHTML Could Allow Information Disclosure (2503658)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0096

Update Details

Recommendation is updated

11770 - (MS11-034) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0662, CVE-2011-0665, CVE-2011-0666, CVE-2011-0667, CVE-2011-0670, CVE-2011-0671, CVE-2011-0672, CVE-2011-0673, CVE-2011-0674, CVE-2011-0676, CVE-2011-0677, CVE-2011-1225, CVE-2011-1226, CVE-2011-1227, CVE-2011-1228, CVE-2011-1229, CVE-2011-1230, CVE-2011-1231, CVE-2011-1232, CVE-2011-1233, CVE-2011-1234, CVE-2011-1235, CVE-2011-1236, CVE-2011-1237, CVE-2011-1238, CVE-2011-1239, CVE-2011-1240, CVE-2011-1241, CVE-2011-1242

Update Details

Recommendation is updated

11789 - (MS11-018) Microsoft Internet Explorer Frame Tag Information Disclosure (2497640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1244

Update Details

Recommendation is updated

11828 - (MS11-018) Microsoft Internet Explorer Javascript Information Disclosure (2497640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1245

Update Details

Recommendation is updated

12207 - (MS11-044) Microsoft Windows .NET Framework Could Allow Remote Code Execution (2538814)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1271

Update Details

Recommendation is updated

12223 - (MS11-051) Vulnerability in Active Directory Certificate Services Web Enrollment Could Allow Elevation of Privilege (2518295)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1264

Update Details

Recommendation is updated

12225 - (MS11-047) Microsoft Hyper-V VMBus Persistent Denial Of Service (2525835)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1872

Update Details

Recommendation is updated

12232 - (MS11-050) Microsoft Internet Explorer MIME Sniffing Information Disclosure (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1246

Update Details

Recommendation is updated

12235 - (MS11-050) Microsoft Internet Explorer toStaticHTML Information Disclosure (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1252

Update Details

Recommendation is updated

12240 - (MS11-050) Microsoft Internet Explorer Drag and Drop Information Disclosure (2530548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1258

Update Details

Recommendation is updated

12243 - (MS11-044) Microsoft Windows .NET Framework Could Allow Remote Code Execution (2538814)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1271

Update Details

Recommendation is updated

12245 - (MS11-051) Microsoft Windows Active Directory Certificate Services Web Enrollment Could Allow Elevation Of Privilege (2518295)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1264

Update Details

Recommendation is updated

12249 - (MS11-047) Microsoft Hyper-V VMBus Persistent Denial Of Service (2525835)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1872

Update Details

Recommendation is updated

12252 - (MS11-037) Vulnerability In MHTML Could Allow Information Disclosure (2544893)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1894

Update Details

Recommendation is updated

12446 - (MS11-057) Microsoft Internet Explorer Event Handlers Information Disclosure (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1960

Update Details

Recommendation is updated

12448 - (MS11-057) Microsoft Internet Explorer Shift JIS Character Encoding Information Disclosure (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1962

Update Details

Recommendation is updated

12457 - (MS11-058) Microsoft DNS Server Uninitialized Memory Corruption Could Allow Remote Code Execution (2562485)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1970

Update Details

Recommendation is updated

12463 - (MS11-061) Microsoft Remote DWA Could Allow Elevation of Privilege (2546250)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1263

Update Details

Recommendation is updated

12470 - (MS11-061) Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1263

Update Details

Recommendation is updated

12472 - (MS11-068) Microsoft Kernel Metadata Parsing Could Allow Denial of Service (2556532)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1971

Update Details

Recommendation is updated

12475 - (MS11-068) Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1971

Update Details

Recommendation is updated

12497 - (MS11-061) Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2011-1263

Update Details

Recommendation is updated

12628 - (MS11-074) Microsoft XSS in SharePoint Calendar Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0653

Update Details

Recommendation is updated

12629 - (MS11-074) Microsoft SharePoint HTML Sanitization Information Disclosure (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1252

Update Details

Recommendation is updated

12630 - (MS11-074) Microsoft SharePoint Editform Script Injection Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1890

Update Details

Recommendation is updated

12631 - (MS11-074) Microsoft SharePoint Contact Details Reflected XSS Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1891

Update Details

Recommendation is updated

12632 - (MS11-074) Microsoft SharePoint Remote File Disclosure Information Disclosure (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1892

Update Details

Recommendation is updated

12633 - (MS11-074) Microsoft SharePoint XSS Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1893

Update Details

Recommendation is updated

12634 - (MS11-074) Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0653, CVE-2011-1252, CVE-2011-1890, CVE-2011-1891, CVE-2011-1892, CVE-2011-1893

Update Details

Recommendation is updated

12739 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k TrueType Font Type Translation (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-2002

Update Details

Recommendation is updated

12759 - (MS11-082) Microsoft Host Integration Server Endless Loop DoS in snabase.exe (2607670)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-2007

Update Details

Recommendation is updated

12760 - (MS11-082) Microsoft Host Integration Server Access of Unallocated Memory DoS (2607670)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-2008

Update Details

Recommendation is updated

12764 - (MS11-082) Vulnerabilities in Host Integration Server Could Allow Denial of Service (2607670)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-2007, CVE-2011-2008

Update Details

Recommendation is updated

13062 - (MS12-006) SSL and TLS Protocols Information Disclosure (2643584)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-3389

Update Details

Recommendation is updated

13063 - (MS11-099) Microsoft Internet Explorer Content-Disposition Information Disclosure (2618444)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-3404

Update Details

Recommendation is updated

13065 - (MS11-099) Microsoft Internet Explorer XSS Filter Information Disclosure (2618444)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1992

Update Details

Recommendation is updated

13160 - (MS11-100) Microsoft .NET Form Authentication Spoofing (2638420)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-3415

Update Details

Recommendation is updated

13190 - (MS12-003) Microsoft Windows CSRSS Elevation of Privilege (2646524)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0005

Update Details

Recommendation is updated

13193 - (MS12-003) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0005

Update Details

Recommendation is updated

13194 - (MS12-006) Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-3389

Update Details

Recommendation is updated

13296 - (MS12-010) Microsoft IE Copy and Paste Information Disclosure (2647516)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0010

Update Details

Recommendation is updated

13298 - (MS12-010) Microsoft IE Null Byte Information Disclosure (2647516)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0012

Update Details

Recommendation is updated

13311 - (MS12-011) Microsoft SharePoint XSS in inplview.aspx (2663841)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0017

Update Details

Recommendation is updated

13312 - (MS12-011) Microsoft SharePoint XSS in themeweb.aspx (2663841)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0144

Update Details

Recommendation is updated

13313 - (MS12-011) Microsoft SharePoint XSS in wizardlist.aspx (2663841)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0145

Update Details

Recommendation is updated

13319 - (MS12-011) Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0017, CVE-2012-0144, CVE-2012-0145

Update Details

Recommendation is updated

13397 - (MS12-017) Microsoft Windows DNS Denial of Service (2647170)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0006

Update Details

Recommendation is updated

13398 - (MS12-017) Vulnerability In DNS Server Could Allow Denial Of Service (2647170)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0006

Update Details

Recommendation is updated

13400 - (MS12-021) Microsoft Visual Studio Add-In Elevation of Privilege (2651019)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0008

Update Details

Recommendation is updated

13401 - (MS12-021) Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0008

Update Details

Recommendation is updated

13623 - (MS12-034) Microsoft Windows .NET Index Comparison Remote Code Execution (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0164

Update Details

Recommendation is updated

13755 - (MS12-037) Microsoft Internet Explorer Scrolling Events Information Disclosure (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1882

Update Details

Recommendation is updated

13762 - (MS12-037) Microsoft Internet Explorer Null Byte Information Disclosure (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1873

Update Details

Recommendation is updated

13763 - (MS12-037) Microsoft Internet Explorer EUC-JP Character Encoding Information Disclosure (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1872

Update Details

Recommendation is updated

13765 - (MS12-037) Microsoft Internet Explorer HTML Sanitization Information Disclosure (2699988)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

Update Details

Recommendation is updated

13779 - (MS12-041) Microsoft Windows Win32k.sys Race Condition Privilege Escalation (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1868

Update Details

Recommendation is updated

13783 - (MS12-039) Microsoft Windows HTML Sanitization Information Disclosure (2707956)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

Update Details

Recommendation is updated

13864 - (MS12-050) Microsoft SharePoint HTML Sanitization Information Disclosure (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

Update Details

Recommendation is updated

13865 - (MS12-050) Microsoft SharePoint Scriptresx.ashx Cross Site Scripting Privilege Escalation (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1859

Update Details

Recommendation is updated

13866 - (MS12-050) Microsoft SharePoint Search Scope Information Disclosure (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1860

Update Details

Recommendation is updated

13867 - (MS12-050) Microsoft SharePoint Script In Username Privilege Escalation (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1861

Update Details

Recommendation is updated

13868 - (MS12-050) Microsoft SharePoint URL Redirection Information Disclosure (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1862

Update Details

Recommendation is updated

13869 - (MS12-050) Microsoft SharePoint Reflected List Parameter Privilege Escalation (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1863

Update Details

Recommendation is updated

13870 - (MS12-050) Vulnerabilities In Microsoft SharePoint Could Allow Elevation Of Privilege (2695502)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858, CVE-2012-1859, CVE-2012-1860, CVE-2012-1861, CVE-2012-1862, CVE-2012-1863

Update Details

Recommendation is updated

13871 - (MS12-046) Microsoft Visual Basic For Applications Insecure Library Loading Remote Code Execution (2707960)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1854

Update Details

Recommendation is updated

13874 - (MS12-049) Microsoft Windows TLS Protocol Information Disclosure (2655992)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1870

Update Details

Recommendation is updated

13876 - (MS12-049) Vulnerability in TLS Could Allow Information Disclosure (2655992)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1870

Update Details

Recommendation is updated

14024 - (MS12-054) Microsoft Windows Networking Components Remote Administration Protocol Denial Of Service (2733594)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1850

Update Details

Recommendation is updated

14130 - (MS12-061) Microsoft Visual Studio Team Foundation Cross Site Scripting Privilege Escalation (2719584)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1892

Update Details

Recommendation is updated

14131 - (MS12-061) Vulnerability in Visual Studio Team Foundation Server Could Allow Elevation of Privilege (2719584)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1892

Update Details

Recommendation is updated

14206 - (MS12-066) Microsoft Office HTML Sanitization Privilege Escalation (2741517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2520

Update Details

Recommendation is updated

14213 - (MS12-070) Microsoft SQL Server Reflected XSS Privilege Escalation (2754849)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2552

Update Details

Recommendation is updated

14214 - (MS12-070) Vulnerability in SQL Server Could Allow Elevation of Privilege (2754849)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2552

Update Details

Recommendation is updated

14216 - (MS12-069) Microsoft Kerberos NULL Dereference Denial Of Service (2754673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2551

Update Details

Recommendation is updated

14217 - (MS12-069) Vulnerability in Kerberos Could Allow Denial of Service (2743555)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2551

Update Details

Recommendation is updated

14363 - (MS12-073) Microsoft Internet Information Services FTP Command Injection Information Disclosure (2733829)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2532

Update Details

Recommendation is updated

14365 - (MS12-073) Vulnerabilities In Microsoft Internet Information Services (IIS) Could Allow Information Disclosure (2733829)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2531, CVE-2012-2532

Update Details

Recommendation is updated

14367 - (MS12-074) Microsoft .NET Framework Code Access Security Information Disclosure (2745030)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1896

Update Details

Recommendation is updated

14487 - (MS12-083) Important Vulnerability in IP-HTTPS Component Could Allow Security Feature Bypass (2765809)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2549

Update Details

Recommendation is updated

14488 - (MS12-083) Microsoft Windows IPHTTPS Revoked Certificate Security Bypass (2765809)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2549

Update Details

Recommendation is updated

14567 - (MS13-004) Microsoft .Net Framework System Drawing Information Disclosure (2769324)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0001

Update Details

Recommendation is updated

14577 - (MS13-006) Microsoft Windows SSL And TLS Protocol Security Bypass (2785220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0013

Update Details

Recommendation is updated

14580 - (MS13-006) Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0013

Update Details

Recommendation is updated

14675 - (MS13-016) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2778344)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1248, CVE-2013-1249, CVE-2013-1250, CVE-2013-1251, CVE-2013-1252, CVE-2013-1253, CVE-2013-1254, CVE-2013-1255, CVE-2013-1256, CVE-2013-1257, CVE-2013-1258, CVE-2013-1259, CVE-2013-1260, CVE-2013-1261, CVE-2013-1262, CVE-2013-1263, CVE-2013-1264, CVE-2013-1265, CVE-2013-1266, CVE-2013-1267, CVE-2013-1268, CVE-2013-1269, CVE-2013-1270, CVE-2013-1271, CVE-2013-1272, CVE-2013-1273, CVE-2013-1274, CVE-2013-1275, CVE-2013-1276, CVE-2013-1277

Update Details

Recommendation is updated

14680 - (MS13-016) Microsoft Windows Race Condition I Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1248

Update Details

Recommendation is updated

14681 - (MS13-016) Microsoft Windows Race Condition II Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1249

Update Details

Recommendation is updated

14682 - (MS13-016) Microsoft Windows Race Condition III Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1250

Update Details

Recommendation is updated

14683 - (MS13-016) Microsoft Windows Race Condition IV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1251

Update Details

Recommendation is updated

14685 - (MS13-016) Microsoft Windows Race Condition IX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1256

Update Details

Recommendation is updated

14686 - (MS13-016) Microsoft Windows Race Condition V Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1252

Update Details

Recommendation is updated

14687 - (MS13-016) Microsoft Windows Race Condition VI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1253

Update Details

Recommendation is updated

14689 - (MS13-016) Microsoft Windows Race Condition VII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1254

Update Details

Recommendation is updated

14691 - (MS13-016) Microsoft Windows Race Condition XXX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1277

Update Details

Recommendation is updated

14692 - (MS13-016) Microsoft Windows Race Condition XXVIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1275

Update Details

Recommendation is updated

14694 - (MS13-016) Microsoft Windows Race Condition XXVII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1274

Update Details

Recommendation is updated

14705 - (MS13-009) Microsoft Internet Explorer Shift JIS Character Encoding Information Disclosure (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0015

Update Details

Recommendation is updated

14708 - (MS13-016) Microsoft Windows Race Condition VIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1255

Update Details

Recommendation is updated

14709 - (MS13-016) Microsoft Windows Race Condition X Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1257

Update Details

Recommendation is updated

14710 - (MS13-016) Microsoft Windows Race Condition XI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1258

Update Details

Recommendation is updated

14720 - (MS13-016) Microsoft Windows Race Condition XII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1259

Update Details

Recommendation is updated

14721 - (MS13-016) Microsoft Windows Race Condition XIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1260

Update Details

Recommendation is updated

14722 - (MS13-016) Microsoft Windows Race Condition XIV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1261

Update Details

Recommendation is updated

14723 - (MS13-016) Microsoft Windows Race Condition XIX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1266

Update Details

Recommendation is updated

14724 - (MS13-016) Microsoft Windows Race Condition XV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1262

Update Details

Recommendation is updated

14725 - (MS13-016) Microsoft Windows Race Condition XVI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1263

Update Details

Recommendation is updated

14726 - (MS13-016) Microsoft Windows Race Condition XVII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1264

Update Details

Recommendation is updated

14727 - (MS13-016) Microsoft Windows Race Condition XVIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1265

Update Details

Recommendation is updated

14728 - (MS13-016) Microsoft Windows Race Condition XX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1267

Update Details

Recommendation is updated

14729 - (MS13-016) Microsoft Windows Race Condition XXI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1268

Update Details

Recommendation is updated

14730 - (MS13-016) Microsoft Windows Race Condition XXII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1269

Update Details

Recommendation is updated

14731 - (MS13-016) Microsoft Windows Race Condition XXIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1270

Update Details

Recommendation is updated

14732 - (MS13-016) Microsoft Windows Race Condition XXIV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1271

Update Details

Recommendation is updated

14733 - (MS13-016) Microsoft Windows Race Condition XXIX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1276

Update Details

Recommendation is updated

14734 - (MS13-016) Microsoft Windows Race Condition XXV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1272

Update Details

Recommendation is updated

14736 - (MS13-016) Microsoft Windows Race Condition XXVI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1273

Update Details

Recommendation is updated

14824 - (MS13-025) Vulnerability in Microsoft OneNote Could Allow Information Disclosure (2816264)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0086

Update Details

Recommendation is updated

14842 - (MS13-025) Microsoft OneNote Buffer Size Validation Information Disclosure (2816264)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0086

Update Details

Recommendation is updated

14929 - (MS13-036) Microsoft Windows Kernel Race Condition I Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1283

Update Details

Recommendation is updated

14931 - (MS13-036) Microsoft Windows Kernel Race Condition II Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1292

Update Details

Recommendation is updated

14932 - (MS13-036) Microsoft Windows Kernel NTFS Pointer Dereference Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1293

Update Details

Recommendation is updated

14933 - (MS13-031) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1284, CVE-2013-1294

Update Details

Recommendation is updated

14935 - (MS13-031) Microsoft Windows Kernel Race Condition I Privilege Escalation (2813170)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1284

Update Details

Recommendation is updated

14936 - (MS13-031) Microsoft Windows Kernel Race Condition II Privilege Escalation (2813170)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1294

Update Details

Recommendation is updated

14940 - (MS13-032) Microsoft Windows Active Directory Memory Consumption Denial of Service (2830914)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1282

Update Details

Recommendation is updated

14941 - (MS13-032) Vulnerability In Active Directory Could Lead To Denial Of Service (2830914)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1282

Update Details

Recommendation is updated

14944 - (MS13-035) Microsoft Server Software And Office Apps HTML Sanitization Privilege Escalation (2821818)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1289

Update Details

Recommendation is updated

14945 - (MS13-035) Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1289

Update Details

Recommendation is updated

14946 - (MS13-030) Microsoft Sharepoint Access Rights Privilege Escalation (2827663)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1290

Update Details

Recommendation is updated

14947 - (MS13-030) Vulnerability in SharePoint Could Allow Information Disclosure (2827663)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1290

Update Details

Recommendation is updated

15035 - (MS13-044) Vulnerability In Microsoft Visio Could Allow Information Disclosure (2834692)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1301

Update Details

Recommendation is updated

15036 - (MS13-044) Microsoft Office Visio XML External Entities Resolution Information Disclosure (2834692)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1301

Update Details

Recommendation is updated

15042 - (MS13-039) Vulnerability in HTTP.sys Could Allow Denial of Service (2829254)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1305

Update Details

Recommendation is updated

15045 - (MS13-039) Microsoft Windows HTTP.sys Denial of Service (2829254)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1305

Update Details

Recommendation is updated

15051 - (MS13-037) Microsoft Internet Explorer JSON Array Information Disclosure (2829530)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1297

Update Details

Recommendation is updated

15056 - (MS13-040) Microsoft .NET Framework XML Digital Signature Spoofing (2836440)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1336

Update Details

Recommendation is updated

15182 - (MS13-048) Microsoft Windows Kernel Information Disclosure (2839229)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3136

Update Details

Recommendation is updated

15183 - (MS13-048) Vulnerability in Windows Kernel Could Allow Information Disclosure (2839229)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3136

Update Details

Recommendation is updated

15257 - (MS13-053) Microsoft Windows Kernel Buffer Overflow Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3172

Update Details

Recommendation is updated

15361 - (MS13-065) Microsoft Windows ICMPv6 Denial of Service (2868623)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3183

Update Details

Recommendation is updated

15363 - (MS13-061) Microsoft Exchange Server Oracle Outside In Technologies Remote Code Execution III (2876063)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3781

Update Details

Recommendation is updated

15364 - (MS13-061) Microsoft Exchange Server Oracle Outside In Technologies Remote Code Execution II (2876063)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3776

Update Details

Recommendation is updated

15366 - (MS13-061) Microsoft Exchange Server Oracle Outside In Technologies Remote Code Execution I (2876063)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-2393

Update Details

Recommendation is updated

15368 - (MS13-064) Microsoft Windows NAT Server Denial of Service (2849568)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3182

Update Details

Recommendation is updated

15369 - (MS13-066) Vulnerability In Active Directory Federation Services Could Allow Information Disclosure (2873872)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3185

Update Details

Recommendation is updated

15370 - (MS13-066) Microsoft Active Directory Federation Services Information Disclosure (2873872)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3185

Update Details

Recommendation is updated

15371 - (MS13-063) Microsoft Windows Kernel Memory Corruption III Remote Code Execution (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3198

Update Details

Recommendation is updated

15372 - (MS13-063) Microsoft Windows Kernel Memory Corruption II Remote Code Execution (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3197

Update Details

Recommendation is updated

15373 - (MS13-063) Microsoft Windows Kernel Memory Corruption I Remote Code Execution (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3196

Update Details

Recommendation is updated

15374 - (MS13-063) Microsoft Windows Kernel ASLR Security Bypass (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-2556

Update Details

Recommendation is updated

15376 - (MS13-059) Microsoft Internet Explorer EUC-JP Character Encoding Information Disclosure (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3192

Update Details

Recommendation is updated

15377 - (MS13-059) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3184

Update Details

Recommendation is updated

15378 - (MS13-059) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3187

Update Details

Recommendation is updated

15379 - (MS13-059) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3188

Update Details

Recommendation is updated

15380 - (MS13-059) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3189

Update Details

Recommendation is updated

15381 - (MS13-059) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3199

Update Details

Recommendation is updated

15382 - (MS13-059) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3190

Update Details

Recommendation is updated

15383 - (MS13-059) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3191

Update Details

Recommendation is updated

15384 - (MS13-059) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3193

Update Details

Recommendation is updated

15385 - (MS13-059) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3194

Update Details

Recommendation is updated

15386 - (MS13-059) Microsoft Internet Explorer Process Integrity Level Assignment Privilege Escalation (2862772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3186

Update Details

Recommendation is updated

15536 - (MS13-072) Microsoft Office XML External Entities Resolution Information Disclosure (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3160

Update Details

Recommendation is updated

15541 - (MS13-067) Microsoft SharePoint Denial of Service (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0081

Update Details

Recommendation is updated

15543 - (MS13-067) Microsoft SharePoint Cross-Site Scripting Privilege Escalation (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3179

Update Details

Recommendation is updated

15544 - (MS13-067) Microsoft SharePoint POST Cross-Site Scripting Privilege Escalation (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3180

Update Details

Recommendation is updated

15549 - (MS13-067) Microsoft SharePoint Office Memory Corruption I Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1315

Update Details

Recommendation is updated

15550 - (MS13-067) Microsoft SharePoint Word Memory Corruption I Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3847

Update Details

Recommendation is updated

15551 - (MS13-067) Microsoft SharePoint Word Memory Corruption II Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3848

Update Details

Recommendation is updated

15552 - (MS13-067) Microsoft SharePoint Word Memory Corruption III Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3849

Update Details

Recommendation is updated

15553 - (MS13-067) Microsoft SharePoint Word Memory Corruption IV Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3857

Update Details

Recommendation is updated

15554 - (MS13-067) Microsoft SharePoint Word Memory Corruption V Remote Code Execution (2834052)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3858

Update Details

Recommendation is updated

15557 - (MS13-072) Microsoft Office Word Memory Corruption I Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3847

Update Details

Recommendation is updated

15559 - (MS13-072) Microsoft Office Word Memory Corruption II Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3848

Update Details

Recommendation is updated

15560 - (MS13-072) Microsoft Office Word Memory Corruption III Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3849

Update Details

Recommendation is updated

15561 - (MS13-072) Microsoft Office Word Memory Corruption IV Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3850

Update Details

Recommendation is updated

15563 - (MS13-072) Microsoft Office Word Memory Corruption V Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3851

Update Details

Recommendation is updated

15564 - (MS13-072) Microsoft Office Word Memory Corruption VI Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3852

Update Details

Recommendation is updated

15565 - (MS13-072) Microsoft Office Word Memory Corruption VII Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3853

Update Details

Recommendation is updated

15566 - (MS13-072) Microsoft Office Word Memory Corruption VIII Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3854

Update Details

Recommendation is updated

15567 - (MS13-072) Microsoft Office Word Memory Corruption IX Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3855

Update Details

Recommendation is updated

15568 - (MS13-072) Microsoft Office Word Memory Corruption X Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3856

Update Details

Recommendation is updated

15570 - (MS13-072) Microsoft Office Word Memory Corruption XI Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3857

Update Details

Recommendation is updated

15571 - (MS13-072) Microsoft Office Word Memory Corruption XII Remote Code Execution (2845537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3858

Update Details

Recommendation is updated

15572 - (MS13-078) Microsoft FrontPage XML Information Disclosure (2825621)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3137

Update Details

Recommendation is updated

15573 - (MS13-078) Vulnerability In FrontPage Could Allow Information Disclosure (2825621)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3137

Update Details

Recommendation is updated

15578 - (MS13-071) Microsoft Windows Theme File Remote Code Execution (2864063)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0810

Update Details

Recommendation is updated

15579 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation I (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1341

Update Details

Recommendation is updated

15580 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation II (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1342

Update Details

Recommendation is updated

15581 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation III (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1343

Update Details

Recommendation is updated

15582 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation IV (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1344

Update Details

Recommendation is updated

15583 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation V (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3864

Update Details

Recommendation is updated

15584 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation VI (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3865

Update Details

Recommendation is updated

15585 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation VII (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3866

Update Details

Recommendation is updated

15586 - (MS13-071) Vulnerability in Windows Theme File Could Allow Remote Code Execution (2864063)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0810

Update Details

Recommendation is updated

15587 - (MS13-077) Microsoft Windows Service Control Manager Double Free Privilege Escalation (2872339)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3862

Update Details

Recommendation is updated

15589 - (MS13-077) Microsoft Windows Service Control Manager Double Free Privilege Escalation (2872339)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3862

Update Details

Recommendation is updated

15590 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution II (2858300)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3158

Update Details

Recommendation is updated

15592 - (MS13-073) Microsoft Office XML External Entities Resolution Information Disclosure (2858300)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3159

Update Details

Recommendation is updated

15598 - (MS13-079) Microsoft Windows Remote Anonymous Persistent Denial of Service (2853587)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3868

Update Details

Recommendation is updated

15599 - (MS13-079) Vulnerability in Active Directory Could Allow Denial of Service (2853587)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3868

Update Details

Recommendation is updated

15704 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution II (2885080)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3890

Update Details

Recommendation is updated

15706 - (MS13-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3872

Update Details

Recommendation is updated

15707 - (MS13-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3873

Update Details

Recommendation is updated

15708 - (MS13-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3874

Update Details

Recommendation is updated

15709 - (MS13-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3875

Update Details

Recommendation is updated

15710 - (MS13-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3882

Update Details

Recommendation is updated

15712 - (MS13-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3885

Update Details

Recommendation is updated

15713 - (MS13-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3886

Update Details

Recommendation is updated

15714 - (MS13-087) Microsoft Silverlight Information Disclosure (2890788)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3896

Update Details

Recommendation is updated

15715 - (MS13-080) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3897

Update Details

Recommendation is updated

15716 - (MS13-080) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2879017)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3893

Update Details

Recommendation is updated

15722 - (MS13-084) Microsoft SharePoint Excel Remote Code Execution (2885089)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3889

Update Details

Recommendation is updated

15723 - (MS13-084) Microsoft SharePoint Parameter Injection Privilege escalation (2885089)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3895

Update Details

Recommendation is updated

15730 - (MS13-082) Microsoft .NET Framework JSON Parsing Denial of Service (2878890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3861

Update Details

Recommendation is updated

15731 - (MS13-082) Microsoft .NET Framework Entity Expansion Denial of Service (2878890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3860

Update Details

Recommendation is updated

15732 - (MS13-082) Microsoft .NET Framework OpenType Font Remote Code Execution (2878890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3128

Update Details

Recommendation is updated

15735 - (MS13-081) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3888

Update Details

Recommendation is updated

15736 - (MS13-081) Microsoft Windows Win32k NULL Page Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3881

Update Details

Recommendation is updated

15737 - (MS13-081) Microsoft Windows App Container Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3880

Update Details

Recommendation is updated

15738 - (MS13-081) Microsoft Windows Win32k Use After Free Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE 2013-3879

Update Details

Recommendation is updated

15739 - (MS13-081) Microsoft Windows USB Descriptor Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3200

Update Details

Recommendation is updated

15907 - (MS13-095) Microsoft Windows XML Digital Signatures Denial of Service (2868626)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3869

Update Details

Recommendation is updated

15908 - (MS13-095) Vulnerability in XML Digital Signatures Could Allow Denial of Service (2868626)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3869

Update Details

Recommendation is updated

15913 - (MS13-094) Microsoft Outlook S/MIME AIA Information Disclosure (2894514)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3905

Update Details

Recommendation is updated

15914 - (MS13-094) Vulnerability In Microsoft Outlook Could Allow Information Disclosure (2894514)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3905

Update Details

Recommendation is updated

15915 - (MS13-092) Vulnerability In Hyper-V Could Allow Elevation of Privilege (2893986)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3898

Update Details

Recommendation is updated

15916 - (MS13-092) Microsoft Windows Hyper-V Address Corruption Privilege Escalation (2893986)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3898

Update Details

Recommendation is updated

15917 - (MS13-088) Microsoft Internet Explorer CSS Characters Information Disclosure (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3909

Update Details

Recommendation is updated

15918 - (MS13-088) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3910

Update Details

Recommendation is updated

15919 - (MS13-088) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3911

Update Details

Recommendation is updated

15920 - (MS13-088) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3912

Update Details

Recommendation is updated

15921 - (MS13-088) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3914

Update Details

Recommendation is updated

15922 - (MS13-088) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3915

Update Details

Recommendation is updated

15923 - (MS13-088) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3916

Update Details

Recommendation is updated

15924 - (MS13-088) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3917

Update Details

Recommendation is updated

15925 - (MS13-088) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3871

Update Details

Recommendation is updated

15926 - (MS13-088) Microsoft Internet Explorer Print Preview Information Disclosure (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3908

Update Details

Recommendation is updated

15929 - (MS13-091) Microsoft Office Word Buffer Overflow Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1324

Update Details

Recommendation is updated

15930 - (MS13-091) Microsoft Office Word Heap Overwrite Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1325

Update Details

Recommendation is updated

15931 - (MS13-091) Microsoft Office WPD File Format Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0082

Update Details

Recommendation is updated

16016 - (MS13-106) Vulnerability In A Microsoft Office Shared Component Could Allow Security Feature Bypass (2905238)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5057

Update Details

Recommendation is updated

16017 - (MS13-106) Microsoft Office HDXS ASLR Security Bypass (2905238)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5057

Update Details

Recommendation is updated

16021 - (MS13-097) Microsoft Internet Explorer Memory Corruption I Privilege Escalation (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5045

Update Details

Recommendation is updated

16022 - (MS13-097) Microsoft Internet Explorer Memory Corruption II Privilege Escalation (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5046

Update Details

Recommendation is updated

16025 - (MS13-104) Vulnerability in Microsoft Office Could Allow Information Disclosure (2909976)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5054

Update Details

Recommendation is updated

16032 - (MS13-105) Microsoft Exchange Oracle Outside In Technologies Remote Code Execution (2915705)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5763

Update Details

Recommendation is updated

16033 - (MS13-101) Microsoft Windows Integer Overflow I Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3899

Update Details

Recommendation is updated

16034 - (MS13-101) Microsoft Windows Use-After-Free Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3902

Update Details

Recommendation is updated

16035 - (MS13-101) Microsoft Windows TrueType Font Parsing Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3903

Update Details

Recommendation is updated

16036 - (MS13-101) Microsoft Windows Port-Class Driver Double Fetch Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3907

Update Details

Recommendation is updated

16037 - (MS13-101) Microsoft Windows Integer Overflow II Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5058

Update Details

Recommendation is updated

16038 - (MS13-104) Microsoft Office Token Hijacking Information Disclosure (2909976)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5054

Update Details

Recommendation is updated

16041 - (MS13-098) Microsoft Windows WinVerifyTrust Signature Validation Remote Code Execution (2893294)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3900

Update Details

Recommendation is updated

16058 - (MS13-105) Microsoft Exchange OWA XSS Remote Code Execution (2915705)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5072

Update Details

Recommendation is updated

16059 - (MS13-105) Microsoft Exchange Oracle Outside In Technologies II Remote Code Execution (2915705)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5791

Update Details

Recommendation is updated

16096 - (MS13-103) Microsoft ASP. NET SignalR XSS Privilege Escalation (2905244)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5042

Update Details

Recommendation is updated

16208 - (MS14-003) Microsoft Windows Kernel-Mode Drivers Privilege Elevation (2913602)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0262

Update Details

Recommendation is updated

16214 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution I (2916605)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0258

Update Details

Recommendation is updated

16215 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution II (2916605)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0259

Update Details

Recommendation is updated

16216 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution III (2916605)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0260

Update Details

Recommendation is updated

16289 - (MS14-010) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0267

Update Details

Recommendation is updated

16290 - (MS14-010) Microsoft Internet Explorer Memory Corruption Privilege Escalation (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0268

Update Details

Recommendation is updated

16291 - (MS14-010) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0269

Update Details

Recommendation is updated

16292 - (MS14-010) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0270

Update Details

Recommendation is updated

16293 - (MS14-010) Microsoft Internet Explorer VBScript Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0271

Update Details

Recommendation is updated

16294 - (MS14-010) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0272

Update Details

Recommendation is updated

16295 - (MS14-010) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0273

Update Details

Recommendation is updated

16296 - (MS14-010) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0274

Update Details

Recommendation is updated

16297 - (MS14-010) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0275

Update Details

Recommendation is updated

16298 - (MS14-010) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0276

Update Details

Recommendation is updated

16299 - (MS14-010) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0277

Update Details

Recommendation is updated

16300 - (MS14-010) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0278

Update Details

Recommendation is updated

16301 - (MS14-010) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0279

Update Details

Recommendation is updated

16302 - (MS14-010) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0280

Update Details

Recommendation is updated

16304 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0283

Update Details

Recommendation is updated

16305 - (MS14-010) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0284

Update Details

Recommendation is updated

16306 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0285

Update Details

Recommendation is updated

16307 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0286

Update Details

Recommendation is updated

16308 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0287

Update Details

Recommendation is updated

16309 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0288

Update Details

Recommendation is updated

16310 - (MS14-010) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0289

Update Details

Recommendation is updated

16311 - (MS14-010) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0290

Update Details

Recommendation is updated

16312 - (MS14-010) Microsoft Internet Explorer Cross Domain Information Disclosure (2909921)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0293

Update Details

Recommendation is updated

16314 - (MS14-006) Microsoft Windows TCP/IP Version 6 Denial of Service (2904659)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0254

Update Details

Recommendation is updated

16318 - (MS14-009) Microsoft .NET Address Space Layout Randomization Security Bypass (2916607)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0295

Update Details

Recommendation is updated

16319 - (MS14-009) Microsoft .NET POST Request Denial of Service (2916607)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0253

Update Details

Recommendation is updated

16320 - (MS14-009) Microsoft .NET Type Traversal Privilege Escalation (2916607)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0257

Update Details

Recommendation is updated

16328 - (MS14-005) Microsoft XML Core Services Information Disclosure (2916036)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0266

Update Details

Recommendation is updated

16403 - (MS14-016) Microsoft SAMR Feature Security Bypass (2934418)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0317

Update Details

Recommendation is updated

16404 - (MS14-016) Vulnerability in Microsoft Remote Protocol Could Allow Security Feature Bypass (2934418)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0317

Update Details

Recommendation is updated

16484 - (MS14-018) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2950467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0235

Update Details

Recommendation is updated

16485 - (MS14-018) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2950467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1751

Update Details

Recommendation is updated

16486 - (MS14-018) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2950467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1752

Update Details

Recommendation is updated

16487 - (MS14-018) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2950467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1753

Update Details

Recommendation is updated

16488 - (MS14-018) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2950467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1755

Update Details

Recommendation is updated

16489 - (MS14-018) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2950467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1760

Update Details

Recommendation is updated

16491 - (MS14-020) Microsoft Publisher Pointer Dereference Remote Code Execution (2950145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1759

Update Details

Recommendation is updated

16493 - (MS14-017) Microsoft Word File Parsing Stack Overflow Remote Code Execution (2949660)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1758

Update Details

Recommendation is updated

16494 - (MS14-017) Microsoft Word File Format Converter Remote Code Execution (2949660)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1757

Update Details

Recommendation is updated

16497 - (MS14-019) Microsoft Windows File Handling Remote Code Execution (2922229)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0315

Update Details

Recommendation is updated

16601 - (MS14-026) Vulnerability in .NET could allow Remote Code Execution (2958732)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1806

Update Details

Recommendation is updated

16602 - (MS14-028) Microsoft Windows iSCSI Target Remote I Denial of Service (2962485)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0255

Update Details

Recommendation is updated

16603 - (MS14-023) Microsoft Office Chinese Grammar Checking Remote Code Execution (2961037)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1756

Update Details

Recommendation is updated

16604 - (MS14-028) Microsoft Windows iSCSI Target Remote II Denial of Service (2962485)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0256

Update Details

Recommendation is updated

16605 - (MS14-023) Microsoft Office Token Reuse Remote Code Execution (2961037)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1808

Update Details

Recommendation is updated

16606 - (MS14-024) Vulnerability in a Microsoft Common Control Could Allow Security Feature Bypass (2961033)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1809

Update Details

Recommendation is updated

16607 - (MS14-028) Vulnerability in iSCSI Could Allow Denial of Service (2962485)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0255, CVE-2014-0256

Update Details

Recommendation is updated

16608 - (MS14-024) Microsoft Common Control ASLR Security Bypass (2961033)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1809

Update Details

Recommendation is updated

16609 - (MS14-029) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2962482)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0310

Update Details

Recommendation is updated

16610 - (MS14-029) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2962482)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1815

Update Details

Recommendation is updated

16611 - (MS14-027) Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (2962488)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1807

Update Details

Recommendation is updated

16612 - (MS14-027) Microsoft Windows Shell Handler File Association Privilege Escalation (2962488)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

16690 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1799

Update Details

Recommendation is updated

16691 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1800

Update Details

Recommendation is updated

16692 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1802

Update Details

Recommendation is updated

16693 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1803

Update Details

Recommendation is updated

16694 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1804

Update Details

Recommendation is updated

16695 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1805

Update Details

Recommendation is updated

16696 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2753

Update Details

Recommendation is updated

16700 - (MS14-030) Vulnerability in Remote Desktop Could Allow Tampering (2969259)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0296

Update Details

Recommendation is updated

16701 - (MS14-033) Vulnerability In Microsoft XML Core Services Could Allow Information Disclosure (2966061)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1816

Update Details

Recommendation is updated

16702 - (MS14-030) Microsoft RDP MAC Tampering Information Disclosure (2969259)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0296

Update Details

Recommendation is updated

16703 - (MS14-033) Microsoft Windows MSXML Entity URI Information Disclosure (2966061)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1816

Update Details

Recommendation is updated

16704 - (MS14-032) Microsoft Lync Server Content Sanitization Information Disclosure (2969258)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1823

Update Details

Recommendation is updated

16706 - (MS14-031) Microsoft Windows TCP Protocol Denial of Service (2962478)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1811

Update Details

Recommendation is updated

16707 - (MS14-032) Vulnerability in Microsoft Lync Server Could Allow Information Disclosure (2969258)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1823

Update Details

Recommendation is updated

16709 - (MS14-034) Microsoft Word Embedded Font Remote Code Execution (2969261)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2778

Update Details

Recommendation is updated

16733 - (MS14-035) Microsoft Internet Explorer Privilege Escalation I (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1764

Update Details

Recommendation is updated

16738 - (MS14-035) Microsoft Internet Explorer Privilege Escalation III (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2777

Update Details

Recommendation is updated

16744 - (MS14-035) Microsoft Internet Explorer Information Disclosure (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1777

Update Details

Recommendation is updated

16745 - (MS14-035) Microsoft Internet Explorer Privilege Escalation II (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1778

Update Details

Recommendation is updated

16759 - (MS14-035) Microsoft Internet Explorer TLS Server Certificate Renegotiation Information Disclosure (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1771

Update Details

Recommendation is updated

16760 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1795

Update Details

Recommendation is updated

16762 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1796

Update Details

Recommendation is updated

16763 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (2969262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1797

Update Details

Recommendation is updated

16840 - (MS14-039) Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege (2975685)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2781

Update Details

Recommendation is updated

16842 - (MS14-041) Microsoft Windows DirectShow Privilege Escalation (2975681)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2780

Update Details

Recommendation is updated

16844 - (MS14-038) Microsoft Windows Journal Remote Code Execution (2975689)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1824

Update Details

Recommendation is updated

16845 - (MS14-037) Microsoft Internet Explorer Extended Validation Certificate Security Bypass (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2783

Update Details

Recommendation is updated

16846 - (MS14-040) Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2975684)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1767

Update Details

Recommendation is updated

16871 - (MS14-039) Microsoft Windows On-Screen Keyboard Privilege Escalation (2975685)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2781

Update Details

Recommendation is updated

16872 - (MS14-040) Microsoft Windows Ancillary Function Driver Privilege Escalation (2975684)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1767

Update Details

Recommendation is updated

16933 - DotNetNuke Multiple Modules Arbitrary File Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

16960 - (MS14-043) Microsoft Windows Media Center CSyncBasePlayer Use After Free Remote Code Execution (2978742)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4060

Update Details

Recommendation is updated

16962 - (MS14-044) Microsoft SQL Server XSS Privilege Escalation (2984340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1820

Update Details

Recommendation is updated

16963 - (MS14-044) Microsoft SQL Server Stack Overrun Privilege Escalation (2984340)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4061

Update Details

Recommendation is updated

16964 - (MS14-047) Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0316

Update Details

Recommendation is updated

16965 - (MS14-047) Microsoft Windows ASLR Bypass Security Bypass (2978668)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0316

Update Details

Recommendation is updated

16969 - (MS14-051) Microsoft Internet Explorer Privilege Escalation II (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2819

Update Details

Recommendation is updated

16970 - (MS14-051) Microsoft Internet Explorer Privilege Escalation I (2976627)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2817

Update Details

Recommendation is updated

16998 - (MS14-045) Microsoft Windows Font Double-Fetch Privilege Escalation (2984615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1819

Update Details

Recommendation is updated

16999 - (MS14-045) Microsoft Windows Kernel Pool Allocation Information Disclosure (2984615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4064

Update Details

Recommendation is updated

17000 - (MS14-045) Microsoft Windows Win32k Privilege Escalation (2984615)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0318

Update Details

Recommendation is updated

17001 - (MS14-046) Microsoft .NET Framework ASLR Security Bypass (2984625)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4062

Update Details

Recommendation is updated

17002 - (MS14-048) Microsoft OneNote File Parsing Remote Code Execution (2977201)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2815

Update Details

Recommendation is updated

17003 - (MS14-049) Microsoft Windows Installer Repair Privilege Escalation (2962490)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1814

Update Details

Recommendation is updated

17004 - (MS14-050) Microsoft Sharepoint Server Page Content Privilege Escalation (2977202)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2816

Update Details

Recommendation is updated

17005 - (MS14-050) Vulnerability in Microsoft SharePoint Server Could Allow Elevation of Privilege (2977202)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2816

Update Details

Recommendation is updated

17010 - (MS14-046) Vulnerability in .NET Framework Could Allow Security Feature Bypass (2984625)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4062

Update Details

Recommendation is updated

17039 - BlackBerry OS OpenSSL Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: Medium

CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

Update Details

Recommendation is updated

17064 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXVI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4111

Update Details

Recommendation is updated

17065 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4110

Update Details

Recommendation is updated

17066 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4109

Update Details

Recommendation is updated

17067 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4108

Update Details

Recommendation is updated

17068 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4107

Update Details

Recommendation is updated

17069 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4106

Update Details

Recommendation is updated

17070 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4105

Update Details

Recommendation is updated

17071 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4104

Update Details

Recommendation is updated

17072 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4103

Update Details

Recommendation is updated

17073 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4102

Update Details

Recommendation is updated

17074 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4101

Update Details

Recommendation is updated

17075 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4100

Update Details

Recommendation is updated

17076 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4099

Update Details

Recommendation is updated

17077 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4098

Update Details

Recommendation is updated

17078 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4097

Update Details

Recommendation is updated

17079 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4096

Update Details

Recommendation is updated

17080 - (MS14-052) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4095

Update Details

Recommendation is updated

17081 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4094

Update Details

Recommendation is updated

17082 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4093

Update Details

Recommendation is updated

17083 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4092

Update Details

Recommendation is updated

17084 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4091

Update Details

Recommendation is updated

17085 - (MS14-052) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4090

Update Details

Recommendation is updated

17086 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4089

Update Details

Recommendation is updated

17087 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4088

Update Details

Recommendation is updated

17088 - (MS14-052) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4087

Update Details

Recommendation is updated

17089 - (MS14-052) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4086

Update Details

Recommendation is updated

17090 - (MS14-052) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4085

Update Details

Recommendation is updated

17091 - (MS14-052) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4084

Update Details

Recommendation is updated

17092 - (MS14-052) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4083

Update Details

Recommendation is updated

17093 - (MS14-052) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4082

Update Details

Recommendation is updated

17094 - (MS14-052) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4081

Update Details

Recommendation is updated

17095 - (MS14-052) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4080

Update Details

Recommendation is updated

17096 - (MS14-052) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4079

Update Details

Recommendation is updated

17097 - (MS14-052) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4065

Update Details

Recommendation is updated

17098 - (MS14-052) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4059

Update Details

Recommendation is updated

17099 - (MS14-052) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-2799

Update Details

Recommendation is updated

17100 - (MS14-052) Microsoft Internet Explorer Resource Anti-Malware Detection Information Disclosure (2977629)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-7331

Update Details

Recommendation is updated

17101 - (MS14-052) Cumulative Security Update for Internet Explorer (2977629)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-7331, CVE-2014-4082, CVE-2014-4083, CVE-2014-4084, CVE-2014-4085, CVE-2014-4086, CVE-2014-4087, CVE-2014-4088, CVE-2014-4089, CVE-2014-4090, CVE-2014-4091, CVE-2014-4092, CVE-2014-4093, CVE-2014-4094, CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4098, CVE-2014-4099, CVE-2014-4100, CVE-2014-4101, CVE-2014-4102, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, CVE-2014-4111

Update Details

Recommendation is updated

17102 - (MS14-054) Microsoft Windows Task Scheduler Integrity Checks Privilege Escalation (2988948)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4074

Update Details

Recommendation is updated

17103 - (MS14-054) Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (2988948)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4074

Update Details

Recommendation is updated

17104 - (MS14-053) Vulnerability in .NET Framework Could Allow Denial of Service (2990931)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4072

Update Details

Recommendation is updated

17105 - (MS14-053) Microsoft .NET Framework ASP.NET Hash Collision Denial of Service (2990931)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4072

Update Details

Recommendation is updated

17106 - (MS14-055) Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service (2990928)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4068, CVE-2014-4070, CVE-2014-4071

Update Details

Recommendation is updated

17107 - (MS14-055) Microsoft Lync Server I Denial of Service (2990928)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4068

Update Details

Recommendation is updated

17108 - (MS14-055) Microsoft Lync Server II Denial of Service (2990928)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4071

Update Details

Recommendation is updated

17109 - (MS14-055) Microsoft Lync Server Cross-Site Scripting Content Sanitizing Information Disclosure (2990928)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4070

Update Details

Recommendation is updated

17149 - (MS13-060) Microsoft Windows Unicode Scripts Font Parsing Remote Code Execution (2850869)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3181

Update Details

Recommendation is updated

17178 - Schneider Electric SCADA Expert ClearSCADA Vulnerabilities

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-5411, CVE-2014-5412, CVE-2014-5413

Update Details

Documentation is updated

17224 - (MS14-057) Microsoft .NET Framework Address Space Layout Randomization Security Bypass (3000414)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4122

Update Details

Recommendation is updated

17226 - (MS14-057) Microsoft .NET Framework ClickOnce Privilege Escalation (3000414)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4073

Update Details

Recommendation is updated

17228 - (MS14-058) Microsoft Windows Win32k.sys Privilege Escalation (3000061)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4113

Update Details

Recommendation is updated

17232 - (MS14-056) Microsoft Internet Explorer I Privilege Escalation (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4123

Update Details

Recommendation is updated

17233 - (MS14-056) Microsoft Internet Explorer II Privilege Escalation (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4124

Update Details

Recommendation is updated

17234 - (MS14-056) Microsoft Internet Explorer ASLR Security Bypass (2987107)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4140

Update Details

Recommendation is updated

17246 - (MS14-060) Microsoft Windows OLE Remote Code Execution (3000869)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4114

Update Details

Recommendation is updated

17247 - (MS14-059) Microsoft ASP.NET MVC Feature Cross-Site Scripting (2990942)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4075

Update Details

Recommendation is updated

17251 - (MS14-059) Vulnerability in ASP.NET MVC Could Allow Security Feature Bypass (2990942)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4075

Update Details

Recommendation is updated

17258 - (MS14-061) Microsoft Word File Format Remote Code Execution (3000434)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4117

Update Details

Recommendation is updated

17261 - (MS14-062) Microsoft Message Queuing Service Arbitrary Write Privilege Escalation (2993254)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4971

Update Details

Recommendation is updated

17263 - (MS14-063) Microsoft Windows Disk Partition Driver Privilege Escalation (2998579)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4115

Update Details

Recommendation is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

Update Details

Recommendation is updated

91623 - Oracle Enterprise Linux ELSA-2014-1671 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3634

Update Details

FASLScript is updated

91628 - Oracle Enterprise Linux ELSA-2014-1676 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-6421, CVE-2014-6422, CVE-2014-6423, CVE-2014-6424, CVE-2014-6425, CVE-2014-6426, CVE-2014-6427, CVE-2014-6428, CVE-2014-6429, CVE-2014-6430, CVE-2014-6431, CVE-2014-6432

Update Details

CVE is updated FASLScript is updated

1989 - (MS02-051) Microsoft Windows RDP Cryptographic Flaw

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0863

Update Details

Recommendation is updated

2130 - (MS02-006) Microsoft Windows 2000 TCP/445 Malformed Packet

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2002-0597

Update Details

Recommendation is updated

2144 - (MS03-031) Microsoft SQL Server 2000 Large Packet

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Medium

CVE: CVE-2003-0231

Update Details

Recommendation is updated

2292 - (MS04-015) Microsoft Windows Help Center Code Execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2004-0199, CVE-2004-0474

Update Details

Recommendation is updated

3894 - (MS05-045) Microsoft Network Connection Manager Denial of Service

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2307

Update Details

Recommendation is updated

3895 - (MS05-044) Microsoft Internet Explorer FTP Client Transfer Location Tampering

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2005-2126

Update Details

Recommendation is updated

4416 - (MS06-031) Microsoft RPC Mutual Authentication Vulnerability (917736)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-2380

Update Details

Recommendation is updated

4665 - (MS06-056) Microsoft .NET Framework 2.0 Cross-Site Scripting Vulnerability (922770)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2006-3436

Update Details

Recommendation is updated

6218 - (MS08-069) Microsoft MSXML DTD Cross-Domain Scripting Vulnerability (955218)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4029

Update Details

Recommendation is updated

6219 - (MS08-069) Microsoft MSXML Chunked Request Vulnerability (955218)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4033

Update Details

Recommendation is updated

7817 - (MS10-035) Microsoft Internet Explorer Cross-Domain Information Disclosure Vulnerability (982381)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0255

Update Details

Recommendation is updated

8708 - Microsoft Office SharePoint 'cid0' Cross-Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2010-0817

Update Details

Recommendation is updated

9083 - (MS10-039) Microsoft Office SharePoint 'cid0' Cross-Site Scripting Vulnerability (983438)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0817

Update Details

Recommendation is updated

9084 - (MS10-039) Microsoft Office Sharepoint Help Page Denial of Service Vulnerability (2028554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1264

Update Details

Recommendation is updated

9697 - (MS10-048) Microsoft Windows Win32k Pool Overflow Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1887

Update Details

Recommendation is updated

9698 - (MS10-048) Microsoft Windows Win32k Bounds Checking Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1887

Update Details

Recommendation is updated

9704 - (MS10-053) Microsoft Internet Explorer Event Handler Cross-Domain Vulnerability (2183461)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1258

Update Details

Recommendation is updated

10038 - (MS10-065) Microsoft IIS Repeated Parameter Request Denial of Service (2267960)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1899

Update Details

Recommendation is updated

10346 - (MS10-071) Microsoft Internet Explorer toStaticHTML Information Disclosure (2360131) I

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3324

Update Details

Recommendation is updated

10347 - (MS10-071) Microsoft Internet Explorer toStaticHTML Information Disclosure (2360131) II

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3243

Update Details

Recommendation is updated

10348 - (MS10-071) Microsoft Internet Explorer CSS Special Character Information Disclosure (2360131)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3325

Update Details

Recommendation is updated

10351 - (MS10-071) Microsoft Internet Explorer Anchor Element Information Disclosure (2360131)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3327

Update Details

Recommendation is updated

10353 - (MS10-071) Microsoft Internet Explorer Cross-Domain Information Disclosure (2360131)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3330

Update Details

Recommendation is updated

10861 - (MS10-106) Vulnerability in Microsoft Exchange Server Could Allow Denial of Service (2407132)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3937

Update Details

Recommendation is updated

10889 - (MS10-106) Microsoft Exchange Server Could Allow Denial of Service (2407132)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3937

Update Details

Recommendation is updated

12231 - (MS11-049) Microsoft XML Editor Could Allow Information Disclosure (2543893)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1280

Update Details

Recommendation is updated

12251 - (MS11-037) Microsoft MHTML Mime-Formatted Request Could Allow Information Disclosure (2544893)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1894

Update Details

Recommendation is updated

12464 - (MS11-066) Microsoft MS Chart Control Could Allow Information Disclosure (2567943)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1977

Update Details

Recommendation is updated

12465 - (MS11-066) Vulnerability in Microsoft Chart Control Could Allow Information Disclosure (2567943)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1977

Update Details

Recommendation is updated

12471 - (MS11-067) Microsoft MS Report Viewer Control XSS Could Allow Information Disclosure (2578230)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1976

Update Details

Recommendation is updated

12473 - (MS11-069) Microsoft .NET Framework Socket Restriction Bypass Could Allow Information Disclosure (2567951)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1978

Update Details

Recommendation is updated

12474 - (MS11-067) Vulnerability in Microsoft Report Viewer Could Allow Information Disclosure (2578230)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1976

Update Details

Recommendation is updated

12476 - (MS11-069) Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1978

Update Details

Recommendation is updated

13404 - (MS12-019) Microsoft Windows DirectWrite Application Denial of Service (2665364)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0156

Update Details

Recommendation is updated

13406 - (MS12-020) Microsoft Terminal Server Denial of Service (2671387)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0152

Update Details

Recommendation is updated

13407 - (MS12-019) Vulnerability in DirectWrite Could Allow Denial of Service (2665364)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0156

Update Details

Recommendation is updated

14205 - (MS12-066) Vulnerabilities in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2520

Update Details

Recommendation is updated

14838 - (MS13-024) Microsoft SharePoint Server JavaScript Elements Privilege Escalation (2780176)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0083

Update Details

Recommendation is updated

15265 - (MS13-055) Microsoft Internet Explorer JIS Character Encoding Remote Code Execution (2846071)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3166

Update Details

Recommendation is updated

15711 - (MS13-087) Vulnerability in Silverlight Could Allow Information Disclosure (2890788)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3896

Update Details

Recommendation is updated

15717 - (MS13-087) Vulnerability in Silverlight Could Allow Information Disclosure (2890788)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-3896

Update Details

Recommendation is updated

16030 - (MS13-103) Vulnerability in ASP.NET SignalR could allow Elevation of Privilege (2905244)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5042

Update Details

Recommendation is updated

33091 - Oracle Solaris 148072-15 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2010-4180, CVE-2013-0166, CVE-2013-0169, CVE-2014-0224, CVE-2014-3508, CVE-2014-3511, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated CVE is updated FASLScript is updated

2050 - (MS03-034) Microsoft Windows NetBIOS Name Service Query Reply Information Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Low

CVE: CVE-2003-0661

Update Details

Recommendation is updated

2109 - (MS03-034) Microsoft Windows NetBIOS Name Service Query Reply Information Disclosure patch

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2003-0661

Update Details

Recommendation is updated

2185 - (MS04-008) Microsoft Windows Media Services DoS

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2003-0905

Update Details

Recommendation is updated

2447 - (MS02-009) Internet Explorer Arbitrary File Accees

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2002-0052

Update Details

Recommendation is updated

4402 - (MS06-029) Microsoft Exchange Server Running Outlook Web Access Vulnerability (912442)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2006-1193

Update Details

Recommendation is updated

4513 - (MS06-043) Microsoft Outlook Express MHTML Parsing Vulnerability (KB920214)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2006-2766

Update Details

Recommendation is updated

6967 - (MS09-036) Microsoft Remote Unauthenticated Denial of Service in ASP.NET Vulnerability (970957)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2009-1536

Update Details

Recommendation is updated

6974 - (MS09-036) Microsoft Remote Unauthenticated Denial of Service in ASP.NET Vulnerability (970957) (Intrusive)

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: Low

CVE: CVE-2009-1536

Update Details

Recommendation is updated

7193 - (MS09-053) IIS FTP Service DoS Vulnerability (975254)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2009-2521

Update Details

Recommendation is updated

7222 - (MS09-053) Vulnerabilities In FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2009-2521

Update Details

Recommendation is updated

7420 - (MS09-036) Vulnerability In ASP.NET In Microsoft Windows Could Allow Denial Of Service (970957)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2009-1536

Update Details

Recommendation is updated

7941 - (MS08-039) Vulnerabilities In Outlook Web Access For Exchange Server Could Allow Elevation Of Privilege (953747)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2008-2247, CVE-2008-2248

Update Details

Recommendation is updated

10345 - (MS10-071) Microsoft Internet Explorer Autocomplete Information Disclosure (2360131)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2010-0808

Update Details

Recommendation is updated

12212 - (MS11-049) Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2011-1280

Update Details

Recommendation is updated

12447 - (MS11-057) Microsoft Internet Explorer Drag And Drop Information Disclosure (2559049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2011-2383

Update Details

Recommendation is updated

14496 - (MS12-080) Microsoft Exchange RSS Feed Handling Denial Of Service (2784126)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-4791

Update Details

Recommendation is updated

14500 - (MS12-080) Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2784126)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3214, CVE-2012-3217, CVE-2012-4791

Update Details

Recommendation is updated

58967 - Debian Linux 7.0 DSA-3045-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-0142, CVE-2014-0143, CVE-2014-0144, CVE-2014-0145, CVE-2014-0146, CVE-2014-0147, CVE-2014-0222, CVE-2014-0223, CVE-2014-3615, CVE-2014-3640

Update Details

FASLScript is updated

142462 - SuSE SLES 11, 11 SP3 rsyslog-9840 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-3634, CVE-2014-3683

Update Details

FASLScript is updated

170338 - Amazon Linux AMI ALAS-2014-370 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-0476

Update Details

Risk is updated

12336 - (MS11-054) Microsoft Windows Win32k Incorrect Parameter Privilege Escalation (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2011-1886

Update Details

Recommendation is updated

13615 - (MS12-032) Microsoft Windows Firewall Security Bypass (2688338)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-0174

Update Details

Recommendation is updated

14025 - (MS12-058) Vulnerabilities in Microsoft Exchange Server WebReady Document Viewing Could Allow Remote Code Execution (2740358)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1766, CVE-2012-1767, CVE-2012-1768, CVE-2012-1769, CVE-2012-1770, CVE-2012-1771, CVE-2012-1772, CVE-2012-1773, CVE-2012-3106, CVE-2012-3107, CVE-2012-3108, CVE-2012-3109, CVE-2012-3110

Update Details

Recommendation is updated

14027 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution I (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1766

Update Details

Recommendation is updated

14028 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution II (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1767

Update Details

Recommendation is updated

14029 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution III (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1768

Update Details

Recommendation is updated

14030 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution IV (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1769

Update Details

Recommendation is updated

14031 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution V (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1770

Update Details

Recommendation is updated

14032 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution VI (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1771

Update Details

Recommendation is updated

14033 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution VII (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1772

Update Details

Recommendation is updated

14034 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution VIII (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1773

Update Details

Recommendation is updated

14035 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution IX (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3106

Update Details

Recommendation is updated

14036 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution X (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3107

Update Details

Recommendation is updated

14037 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution XI (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3108

Update Details

Recommendation is updated

14039 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution XII (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3109

Update Details

Recommendation is updated

14041 - (MS12-058) Microsoft Exchange Server Outside In Filters Remote Code Execution XIII (2740358)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3110

Update Details

Recommendation is updated

14204 - (MS12-067) Vulnerabilities in FAST Search Server 2010 for SharePoint Parsing Could Allow Elevation of Privilege (2742321)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1766, CVE-2012-1767, CVE-2012-1768, CVE-2012-1769, CVE-2012-1770, CVE-2012-1771, CVE-2012-1772 , CVE-2012-1773, CVE-2012-3106, CVE-2012-3107, CVE-2012-3108 , CVE-2012-3109 , CVE-2012-3110

Update Details

Recommendation is updated

14209 - (MS12-067) Vulnerabilities in FAST Search Server 2010 for SharePoint Parsing Could Allow Elevation of Privilege (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1766

Update Details

Recommendation is updated

14220 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation II (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1767

Update Details

Recommendation is updated

14221 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation III (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1768

Update Details

Recommendation is updated

14222 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation IV (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1769

Update Details

Recommendation is updated

14223 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation V (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1770

Update Details

Recommendation is updated

14224 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation VI (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1771

Update Details

Recommendation is updated

14225 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation VII (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1772

Update Details

Recommendation is updated

14226 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation VIII (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-1773

Update Details

Recommendation is updated

14227 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation IX (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3106

Update Details

Recommendation is updated

14228 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation X (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3107

Update Details

Recommendation is updated

14229 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation XI (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3108

Update Details

Recommendation is updated

14230 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation XII (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3109

Update Details

Recommendation is updated

14231 - (MS12-067) Microsoft FAST Server Oracle Outside In Privilege Escalation XIII (2742321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3110

Update Details

Recommendation is updated

14362 - (MS12-073) Microsoft Internet Information Services Password Disclosure Information Disclosure (2733829)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-2531

Update Details

Recommendation is updated

14497 - (MS12-080) Microsoft Exchange Server Oracle Outside In Remote Code Execution I (2784126)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3214

Update Details

Recommendation is updated

14498 - (MS12-080) Microsoft Exchange Server Oracle Outside In Remote Code Execution II (2784126)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2012-3217

Update Details

Recommendation is updated

70046 - macosx.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70072 - general-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70074 - mcafee.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70114 - juniper.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

ADDITIONAL NOTES

- An enhanced recommendation format is applied to Patch Tuesday related content. Recommendations are now including precise superseded logic based on Microsoft Windows Server Update Services, including superseded logic at KB level.
- FSL Version is now included as part of the release notes.

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.