2014-NOV-13
FSL version 7.5.646

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

58995 - Debian Linux 7.0 DSA-3071-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1544

Description

The scan detected that the host is missing the following update:
DSA-3071-1

Observation

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

http://www.debian.org/security/2014/dsa-3071

Debian 7.0
all
libnss3-dbg_2:3.14.5-1+deb7u3
libnss3-dev_2:3.14.5-1+deb7u3
libnss3_2:3.14.5-1+deb7u3
libnss3-1d_2:3.14.5-1+deb7u3
libnss3-tools_2:3.14.5-1+deb7u3

142484 - SuSE SLED 11 SP3 flash-player-9898 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0558, CVE-2014-0564, CVE-2014-0569

Description

The scan detected that the host is missing the following update:
flash-player-9898

Observation

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

https://download.suse.com/Download?buildid=lGGBxW9gbuQ~
https://download.suse.com/Download?buildid=2-fXOLB1uxs~

SuSE SLED 11 SP3
x86_64
flash-player-kde4-11.2.202.411-0.3.1

flash-player-gnome-11.2.202.411-0.3.1
flash-player-11.2.202.411-0.3.1

i586
flash-player-kde4-11.2.202.411-0.3.1
flash-player-gnome-11.2.202.411-0.3.1
flash-player-11.2.202.411-0.3.1

142487 - SuSE Linux 13.1 openSUSE-SU-2014:1378-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3178, 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

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1378-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00025.html

SuSE Linux 13.1
i586
chromium-38.0.2125.104-54.4
chromium-debuginfo-38.0.2125.104-54.4
chromium-ffmpegsumo-debuginfo-38.0.2125.104-54.4
chromedriver-debuginfo-38.0.2125.104-54.4
chromium-ffmpegsumo-38.0.2125.104-54.4
chromium-desktop-kde-38.0.2125.104-54.4
chromium-desktop-gnome-38.0.2125.104-54.4
chromium-debugsource-38.0.2125.104-54.4
chromedriver-38.0.2125.104-54.4

17341 - Opera Multiple Vulnerabilities Prior To 25

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple unspecified vulnerabilities are present in some versions of Opera.

Observation

Opera is a popular web browser.

Multiple unspecified vulnerabilities are present in some versions of Opera. The flaws lie in the embedded Chromium engine.
Successful exploitation could allow an attacker to cause unknown impact.

17353 - Emerson ROCLINK 800 arpro2.dll ActiveX Control Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of Emerson ROCLINK 800 could lead to remote code execution.

Observation

A vulnerability in some versions of Emerson ROCLINK 800 could lead to remote code execution.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

142483 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1380-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1380-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00026.html

SuSE Linux 13.1
i586
wget-1.16-3.4.1
wget-debugsource-1.16-3.4.1
wget-debuginfo-1.16-3.4.1

SuSE Linux 12.3
i586
wget-1.16-15.4.1
wget-debuginfo-1.16-15.4.1
wget-debugsource-1.16-15.4.1

SuSE Linux 13.2
i586
wget-1.16-4.4.1
wget-debugsource-1.16-4.4.1
wget-debuginfo-1.16-4.4.1

142499 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 wget-9933 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

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

wget-9933

Observation

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

https://download.suse.com/Download?buildid=JScJj0sSZk8~
https://download.suse.com/Download?buildid=yb17XbJXVtc~
https://download.suse.com/Download?buildid=Sy9ujYMkupI~
https://download.suse.com/Download?buildid=_EuSwMdl02E~
https://download.suse.com/Download?buildid=O9Hs7WiVrW4~
https://download.suse.com/Download?buildid=raoKR_7edSs~
https://download.suse.com/Download?buildid=I3a3hDlznb4~
https://download.suse.com/Download?buildid=xldVaeDjORk~
https://download.suse.com/Download?buildid=XECbFQuIS34~

SuSE SLED 11 SP3
x86_64
wget-1.11.4-1.19.1

i586
wget-1.11.4-1.19.1

SuSE SLES 11 SP3
x86_64
wget-1.11.4-1.19.1

i586
wget-1.11.4-1.19.1

SuSE SLED 11
x86_64
wget-1.11.4-1.19.1

i586
wget-1.11.4-1.19.1

SuSE SLES 11
x86_64
wget-1.11.4-1.19.1

i586
wget-1.11.4-1.19.1

170413 - Amazon Linux AMI ALAS-2014-442 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
ALAS-2014-442

Observation

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

https://alas.aws.amazon.com/ALAS-2014-442.html

Amazon Linux AMI
x86_64
wget-debuginfo-1.16-1.13.amzn1
wget-1.16-1.13.amzn1

i686
wget-debuginfo-1.16-1.13.amzn1
wget-1.16-1.13.amzn1

177989 - Gentoo Linux GLSA-201411-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-1441, CVE-2010-1442, CVE-2010-1443, CVE-2010-1444, CVE-2010-1445, CVE-2010-2062, CVE-2010-2937, CVE-2010-3124, CVE-2010-3275, CVE-2010-3276, CVE-2010-3907, CVE-2011-0021, CVE-2011-0522, CVE-2011-0531, CVE-2011-1087, CVE-2011-1684, CVE-2011-2194, CVE-2011-2587, CVE-2011-2588, CVE-2011-3623, CVE-2012-0023, CVE-2012-1775, CVE-2012-1776, CVE-2012-2396, CVE-2012-3377, CVE-2012-5470, CVE-2012-5855, CVE-2013-1868, CVE-2013-1954, CVE-2013-3245, CVE-2013-4388, CVE-2013-6283, CVE-2013-6934

Description

The scan detected that the host is missing the following update:
GLSA-201411-01

Observation

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

http://security.gentoo.org/glsa/glsa-201411-01.xml

Affected packages:
media-video/vlc < 2.1.2

181286 - FreeBSD wget Path Traversal Vulnerability In Recursive FTP Mode (ee7b4f9d-66c8-11e4-9ae1-e8e0b722a85e)

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
wget -- path traversal vulnerability in recursive FTP mode (ee7b4f9d-66c8-11e4-9ae1-e8e0b722a85e)

Observation

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

http://www.vuxml.org/freebsd/ee7b4f9d-66c8-11e4-9ae1-e8e0b722a85e.html

Affected packages:
wget < 1.16

17333 - WordPress BuddyPress Plugin Script Insertion And Security Bypass Vulnerabilities

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

Risk Level: High

CVE: CVE-2014-1888, CVE-2014-1889

Description

Multiple vulnerabilities are present in some versions of BuddyPress Plugin for WordPress.

Observation

WordPress is a popular blog web application.

Multiple vulnerabilities are present in some versions of BuddyPress Plugin for WordPress. The flaws lie in multiple parameters which are not being properly sanitized by the plugin. Successful exploitation could allow an attacker to execute arbitrary web code.

17344 - (HPSBMU03123) HP Network Automation Unspecified Security Bypass Vulnerability

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

Risk Level: High

CVE: CVE-2014-2646

Description

A security bypass vulnerability is present in some versions of HP Network Automation.

Observation

HP Network Automation is a network configuration management automation software.

A security bypass vulnerability is present in some versions of HP Network Automation. The flaw is due to an unspecified issue. Successful exploitation could allow an attacker to bypass security restrictions.

17354 - NOVUS NConfig Configurator Unspecified Defect Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of NOVUS NConfig Configurator could lead to remote code execution.

Observation

A vulnerability in some versions of NOVUS NConfig Configurator could lead to remote code execution.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17355 - Moxa MXview Java Applet Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of Moxa MXview could lead to remote code execution.

Observation

A vulnerability in some versions of Moxa MXview could lead to remote code execution.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17414 - LanSweeper Firefox Plugin runApp Method Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of LanSweeper Firefox Plugin could lead to remote code execution.

Observation

A vulnerability in some versions of LanSweeper Firefox Plugin could lead to remote code execution.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

177986 - Gentoo Linux GLSA-201411-02 Update Is Not Installed

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

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

The scan detected that the host is missing the following update:
GLSA-201411-02

Observation

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

http://security.gentoo.org/glsa/glsa-201411-02.xml

Affected packages:
dev-db/mysql < 5.5.40
dev-db/mariadb < 5.5.40-r1

85820 - CentOS 5 CESA-2014-1824 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-3669, CVE-2014-3670, CVE-2014-8626

Description

The scan detected that the host is missing the following update:
CESA-2014-1824

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020743.html

CentOS 5
x86_64
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

i386
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

85821 - CentOS 6 CESA-2014-1826 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-6051, CVE-2014-6052, CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
CESA-2014-1826

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020747.html

CentOS 6
x86_64
libvncserver-0.9.7-7.el6_6.1
libvncserver-devel-0.9.7-7.el6_6.1

i686
libvncserver-0.9.7-7.el6_6.1
libvncserver-devel-0.9.7-7.el6_6.1

85822 - CentOS 6 CESA-2014-1803 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-8566, CVE-2014-8567

Description

The scan detected that the host is missing the following update:
CESA-2014-1803

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020737.html

CentOS 6
x86_64
mod_auth_mellon-0.8.0-3.el6_6

i686
mod_auth_mellon-0.8.0-3.el6_6

91655 - Oracle Enterprise Linux ELSA-2014-1826 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-0904, CVE-2011-0905, CVE-2014-6051, CVE-2014-6052, CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
ELSA-2014-1826

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004627.html
http://oss.oracle.com/pipermail/el-errata/2014-November/004629.html

OEL6
x86_64
libvncserver-0.9.7-7.el6_6.1
libvncserver-devel-0.9.7-7.el6_6.1

i386
libvncserver-0.9.7-7.el6_6.1
libvncserver-devel-0.9.7-7.el6_6.1

OEL7
x86_64
libvncserver-devel-0.9.9-9.el7_0.1
libvncserver-0.9.9-9.el7_0.1

91657 - Oracle Enterprise Linux ELSA-2014-1803 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8566, CVE-2014-8567

Description

The scan detected that the host is missing the following update:
ELSA-2014-1803

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004614.html

OEL6
x86_64
mod_auth_mellon-0.8.0-3.el6_6

i386
mod_auth_mellon-0.8.0-3.el6_6

91658 - Oracle Enterprise Linux ELSA-2014-1801 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3675, CVE-2014-3676, CVE-2014-3677

Description

The scan detected that the host is missing the following update:
ELSA-2014-1801

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004617.html

OEL7
x86_64
shim-0.7-8.0.1.el7_0

shim-unsigned-0.7-8.0.1.el7_0
mokutil-0.7-8.0.1.el7_0

91660 - Oracle Enterprise Linux ELSA-2014-1824 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3669, CVE-2014-3670, CVE-2014-8626

Description

The scan detected that the host is missing the following update:
ELSA-2014-1824

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004623.html

OEL5
x86_64
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

i386
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11

php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

140604 - Red Hat Enterprise Linux RHSA-2014-1803 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8566, CVE-2014-8567

Description

The scan detected that the host is missing the following update:
RHSA-2014-1803

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1803.html

RHEL6S
x86_64
mod_auth_mellon-debuginfo-0.8.0-3.el6_6
mod_auth_mellon-0.8.0-3.el6_6

i386
mod_auth_mellon-debuginfo-0.8.0-3.el6_6
mod_auth_mellon-0.8.0-3.el6_6

RHEL6WS
x86_64
mod_auth_mellon-debuginfo-0.8.0-3.el6_6
mod_auth_mellon-0.8.0-3.el6_6

i386
mod_auth_mellon-debuginfo-0.8.0-3.el6_6
mod_auth_mellon-0.8.0-3.el6_6

140606 - Red Hat Enterprise Linux RHSA-2014-1826 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6051, CVE-2014-6052, CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
RHSA-2014-1826

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1826.html

RHEL7WS
x86_64

libvncserver-0.9.9-9.el7_0.1
libvncserver-debuginfo-0.9.9-9.el7_0.1

RHEL7D
x86_64
libvncserver-0.9.9-9.el7_0.1
libvncserver-debuginfo-0.9.9-9.el7_0.1

RHEL6D
x86_64
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1

i386
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1

RHEL6S
x86_64
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1

i386
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1

RHEL7S
x86_64
libvncserver-0.9.9-9.el7_0.1
libvncserver-debuginfo-0.9.9-9.el7_0.1

RHEL6WS
x86_64
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1

i386
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1

140607 - Red Hat Enterprise Linux RHSA-2014-1824 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3669, CVE-2014-3670, CVE-2014-8626

Description

The scan detected that the host is missing the following update:
RHSA-2014-1824

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1824.html

RHEL5D
x86_64

php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-debuginfo-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

i386
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-debuginfo-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

RHEL5S
x86_64
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-debuginfo-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11

php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

i386
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-debuginfo-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

142488 - SuSE Linux 13.2 openSUSE-SU-2014:1391-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1391-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00034.html

SuSE Linux 13.2
i586
php5-soap-debuginfo-5.6.1-4.1
php5-zlib-5.6.1-4.1
php5-bz2-5.6.1-4.1
php5-xmlrpc-5.6.1-4.1
php5-pspell-debuginfo-5.6.1-4.1
php5-curl-debuginfo-5.6.1-4.1
php5-pear-5.6.1-4.1
php5-devel-5.6.1-4.1
php5-xsl-5.6.1-4.1
php5-dom-5.6.1-4.1
php5-phar-5.6.1-4.1
php5-wddx-5.6.1-4.1

php5-debugsource-5.6.1-4.1
php5-debuginfo-5.6.1-4.1
php5-sysvmsg-5.6.1-4.1
php5-opcache-debuginfo-5.6.1-4.1
php5-mcrypt-5.6.1-4.1
php5-xmlrpc-debuginfo-5.6.1-4.1
php5-tidy-5.6.1-4.1
php5-pdo-5.6.1-4.1
php5-dba-debuginfo-5.6.1-4.1
php5-mssql-debuginfo-5.6.1-4.1
php5-tidy-debuginfo-5.6.1-4.1
php5-pcntl-5.6.1-4.1
php5-sockets-debuginfo-5.6.1-4.1
php5-shmop-debuginfo-5.6.1-4.1
php5-calendar-debuginfo-5.6.1-4.1
php5-posix-5.6.1-4.1
php5-sysvmsg-debuginfo-5.6.1-4.1
php5-fpm-debuginfo-5.6.1-4.1
php5-mysql-debuginfo-5.6.1-4.1
php5-gmp-debuginfo-5.6.1-4.1
php5-xmlreader-debuginfo-5.6.1-4.1
php5-mssql-5.6.1-4.1
php5-zlib-debuginfo-5.6.1-4.1
php5-imap-5.6.1-4.1
php5-gettext-debuginfo-5.6.1-4.1
php5-pdo-debuginfo-5.6.1-4.1
php5-mbstring-5.6.1-4.1
php5-suhosin-debuginfo-5.6.1-4.1
php5-intl-debuginfo-5.6.1-4.1
php5-shmop-5.6.1-4.1
php5-mbstring-debuginfo-5.6.1-4.1
php5-snmp-5.6.1-4.1
php5-ctype-debuginfo-5.6.1-4.1
php5-zip-5.6.1-4.1
php5-sysvsem-debuginfo-5.6.1-4.1
php5-ftp-5.6.1-4.1
php5-exif-debuginfo-5.6.1-4.1
php5-ldap-5.6.1-4.1
php5-dom-debuginfo-5.6.1-4.1
php5-xsl-debuginfo-5.6.1-4.1
php5-openssl-debuginfo-5.6.1-4.1
php5-posix-debuginfo-5.6.1-4.1
php5-pspell-5.6.1-4.1
php5-xmlwriter-5.6.1-4.1
php5-5.6.1-4.1
php5-exif-5.6.1-4.1
php5-iconv-5.6.1-4.1
php5-bz2-debuginfo-5.6.1-4.1
php5-xmlwriter-debuginfo-5.6.1-4.1
php5-ctype-5.6.1-4.1
php5-snmp-debuginfo-5.6.1-4.1
php5-ftp-debuginfo-5.6.1-4.1
php5-fastcgi-5.6.1-4.1
php5-enchant-5.6.1-4.1
php5-curl-5.6.1-4.1
php5-gmp-5.6.1-4.1
apache2-mod_php5-debuginfo-5.6.1-4.1
php5-wddx-debuginfo-5.6.1-4.1
php5-sockets-5.6.1-4.1
php5-firebird-5.6.1-4.1

php5-json-debuginfo-5.6.1-4.1
php5-ldap-debuginfo-5.6.1-4.1
php5-odbc-5.6.1-4.1
php5-mcrypt-debuginfo-5.6.1-4.1
php5-readline-debuginfo-5.6.1-4.1
php5-mysql-5.6.1-4.1
php5-suhosin-5.6.1-4.1
php5-bcmath-5.6.1-4.1
php5-bcmath-debuginfo-5.6.1-4.1
php5-fastcgi-debuginfo-5.6.1-4.1
php5-sqlite-5.6.1-4.1
php5-iconv-debuginfo-5.6.1-4.1
php5-imap-debuginfo-5.6.1-4.1
php5-opcache-5.6.1-4.1
php5-phar-debuginfo-5.6.1-4.1
php5-firebird-debuginfo-5.6.1-4.1
php5-fileinfo-debuginfo-5.6.1-4.1
php5-odbc-debuginfo-5.6.1-4.1
php5-sysvshm-5.6.1-4.1
php5-sqlite-debuginfo-5.6.1-4.1
php5-pgsql-debuginfo-5.6.1-4.1
php5-enchant-debuginfo-5.6.1-4.1
php5-readline-5.6.1-4.1
php5-xmlreader-5.6.1-4.1
php5-gd-debuginfo-5.6.1-4.1
php5-sysvshm-debuginfo-5.6.1-4.1
php5-pgsql-5.6.1-4.1
php5-sysvsem-5.6.1-4.1
php5-fpm-5.6.1-4.1
php5-soap-5.6.1-4.1
php5-tokenizer-debuginfo-5.6.1-4.1
php5-zip-debuginfo-5.6.1-4.1
php5-json-5.6.1-4.1
php5-pcntl-debuginfo-5.6.1-4.1
php5-tokenizer-5.6.1-4.1
php5-fileinfo-5.6.1-4.1
php5-gettext-5.6.1-4.1
php5-calendar-5.6.1-4.1
php5-gd-5.6.1-4.1
php5-openssl-5.6.1-4.1
apache2-mod_php5-5.6.1-4.1
php5-dba-5.6.1-4.1
php5-intl-5.6.1-4.1

142489 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1377-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1377-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00024.html

SuSE Linux 13.1
i586
php5-fileinfo-debuginfo-5.4.20-34.3
php5-suhosin-debuginfo-5.4.20-34.3
php5-posix-debuginfo-5.4.20-34.3
php5-mbstring-5.4.20-34.3
php5-dom-5.4.20-34.3
php5-posix-5.4.20-34.3
php5-pear-5.4.20-34.3
php5-iconv-debuginfo-5.4.20-34.3
php5-calendar-5.4.20-34.3
php5-enchant-5.4.20-34.3
php5-mbstring-debuginfo-5.4.20-34.3
php5-fastcgi-debuginfo-5.4.20-34.3
php5-json-5.4.20-34.3
php5-sqlite-debuginfo-5.4.20-34.3
php5-wddx-5.4.20-34.3
php5-snmp-debuginfo-5.4.20-34.3
php5-iconv-5.4.20-34.3
php5-bcmath-5.4.20-34.3
php5-ldap-debuginfo-5.4.20-34.3
php5-ctype-5.4.20-34.3
php5-gd-5.4.20-34.3
php5-mcrypt-debuginfo-5.4.20-34.3
php5-mysql-debuginfo-5.4.20-34.3
php5-tokenizer-5.4.20-34.3
php5-fileinfo-5.4.20-34.3
php5-shmop-debuginfo-5.4.20-34.3
php5-odbc-debuginfo-5.4.20-34.3
php5-pdo-debuginfo-5.4.20-34.3
php5-bz2-debuginfo-5.4.20-34.3
php5-enchant-debuginfo-5.4.20-34.3
php5-xsl-debuginfo-5.4.20-34.3
php5-xmlwriter-debuginfo-5.4.20-34.3
php5-curl-5.4.20-34.3
php5-debuginfo-5.4.20-34.3
php5-gettext-debuginfo-5.4.20-34.3
php5-devel-5.4.20-34.3
php5-fpm-5.4.20-34.3
php5-zlib-5.4.20-34.3
php5-gd-debuginfo-5.4.20-34.3
apache2-mod_php5-5.4.20-34.3
php5-dba-debuginfo-5.4.20-34.3
php5-bcmath-debuginfo-5.4.20-34.3
php5-odbc-5.4.20-34.3
php5-firebird-debuginfo-5.4.20-34.3
php5-intl-debuginfo-5.4.20-34.3
php5-mssql-debuginfo-5.4.20-34.3
php5-pdo-5.4.20-34.3
php5-pgsql-5.4.20-34.3
php5-zip-5.4.20-34.3
php5-sysvshm-debuginfo-5.4.20-34.3
php5-sockets-debuginfo-5.4.20-34.3
php5-xmlrpc-debuginfo-5.4.20-34.3
php5-mcrypt-5.4.20-34.3
php5-pcntl-5.4.20-34.3
php5-tidy-debuginfo-5.4.20-34.3
php5-shmop-5.4.20-34.3

php5-mysql-5.4.20-34.3
php5-pspell-5.4.20-34.3
php5-wddx-debuginfo-5.4.20-34.3
php5-debugsource-5.4.20-34.3
php5-sockets-5.4.20-34.3
php5-ftp-5.4.20-34.3
php5-intl-5.4.20-34.3
php5-phar-debuginfo-5.4.20-34.3
php5-suhosin-5.4.20-34.3
php5-calendar-debuginfo-5.4.20-34.3
php5-zlib-debuginfo-5.4.20-34.3
php5-phar-5.4.20-34.3
php5-fpm-debuginfo-5.4.20-34.3
php5-gmp-debuginfo-5.4.20-34.3
php5-sysvshm-5.4.20-34.3
php5-sysvmsg-5.4.20-34.3
php5-sqlite-5.4.20-34.3
php5-tidy-5.4.20-34.3
php5-curl-debuginfo-5.4.20-34.3
php5-json-debuginfo-5.4.20-34.3
php5-soap-5.4.20-34.3
php5-mssql-5.4.20-34.3
php5-fastcgi-5.4.20-34.3
php5-soap-debuginfo-5.4.20-34.3
php5-exif-debuginfo-5.4.20-34.3
php5-readline-debuginfo-5.4.20-34.3
php5-firebird-5.4.20-34.3
php5-gettext-5.4.20-34.3
php5-pcntl-debuginfo-5.4.20-34.3
php5-5.4.20-34.3
php5-ftp-debuginfo-5.4.20-34.3
php5-xsl-5.4.20-34.3
php5-readline-5.4.20-34.3
php5-snmp-5.4.20-34.3
php5-openssl-5.4.20-34.3
php5-sysvmsg-debuginfo-5.4.20-34.3
php5-zip-debuginfo-5.4.20-34.3
php5-ctype-debuginfo-5.4.20-34.3
apache2-mod_php5-debuginfo-5.4.20-34.3
php5-bz2-5.4.20-34.3
php5-xmlwriter-5.4.20-34.3
php5-openssl-debuginfo-5.4.20-34.3
php5-xmlreader-5.4.20-34.3
php5-exif-5.4.20-34.3
php5-pgsql-debuginfo-5.4.20-34.3
php5-sysvsem-5.4.20-34.3
php5-xmlrpc-5.4.20-34.3
php5-imap-5.4.20-34.3
php5-dom-debuginfo-5.4.20-34.3
php5-ldap-5.4.20-34.3
php5-dba-5.4.20-34.3
php5-xmlreader-debuginfo-5.4.20-34.3
php5-tokenizer-debuginfo-5.4.20-34.3
php5-sysvsem-debuginfo-5.4.20-34.3
php5-pspell-debuginfo-5.4.20-34.3
php5-imap-debuginfo-5.4.20-34.3
php5-gmp-5.4.20-34.3

SuSE Linux 12.3
i586

php5-bcmath-debuginfo-5.3.17-3.38.2
php5-gmp-debuginfo-5.3.17-3.38.2
php5-sockets-5.3.17-3.38.2
php5-readline-debuginfo-5.3.17-3.38.2
php5-sqlite-5.3.17-3.38.2
php5-wddx-5.3.17-3.38.2
php5-pspell-5.3.17-3.38.2
php5-ftp-5.3.17-3.38.2
php5-pdo-5.3.17-3.38.2
php5-mbstring-5.3.17-3.38.2
php5-sysvsem-5.3.17-3.38.2
php5-pcntl-5.3.17-3.38.2
php5-fileinfo-debuginfo-5.3.17-3.38.2
php5-tidy-debuginfo-5.3.17-3.38.2
php5-shmop-5.3.17-3.38.2
php5-suhosin-debuginfo-5.3.17-3.38.2
php5-xsl-debuginfo-5.3.17-3.38.2
php5-bz2-debuginfo-5.3.17-3.38.2
php5-soap-5.3.17-3.38.2
php5-gmp-5.3.17-3.38.2
php5-zip-debuginfo-5.3.17-3.38.2
php5-fpm-5.3.17-3.38.2
php5-iconv-debuginfo-5.3.17-3.38.2
php5-debuginfo-5.3.17-3.38.2
php5-tokenizer-5.3.17-3.38.2
php5-intl-debuginfo-5.3.17-3.38.2
php5-5.3.17-3.38.2
php5-calendar-debuginfo-5.3.17-3.38.2
php5-ctype-debuginfo-5.3.17-3.38.2
php5-mcrypt-debuginfo-5.3.17-3.38.2
php5-phar-5.3.17-3.38.2
php5-pdo-debuginfo-5.3.17-3.38.2
php5-odbc-debuginfo-5.3.17-3.38.2
php5-fastcgi-5.3.17-3.38.2
php5-iconv-5.3.17-3.38.2
php5-posix-5.3.17-3.38.2
apache2-mod_php5-5.3.17-3.38.2
php5-zlib-5.3.17-3.38.2
php5-pgsql-5.3.17-3.38.2
php5-openssl-5.3.17-3.38.2
php5-dba-5.3.17-3.38.2
php5-dba-debuginfo-5.3.17-3.38.2
php5-fileinfo-5.3.17-3.38.2
php5-ctype-5.3.17-3.38.2
php5-shmop-debuginfo-5.3.17-3.38.2
php5-sysvmsg-debuginfo-5.3.17-3.38.2
php5-zip-5.3.17-3.38.2
php5-xmlwriter-debuginfo-5.3.17-3.38.2
php5-xmlreader-5.3.17-3.38.2
php5-phar-debuginfo-5.3.17-3.38.2
php5-sysvmsg-5.3.17-3.38.2
php5-ldap-debuginfo-5.3.17-3.38.2
php5-xsl-5.3.17-3.38.2
php5-debugsource-5.3.17-3.38.2
php5-exif-debuginfo-5.3.17-3.38.2
php5-dom-5.3.17-3.38.2
php5-imap-debuginfo-5.3.17-3.38.2
php5-posix-debuginfo-5.3.17-3.38.2
php5-pgsql-debuginfo-5.3.17-3.38.2
php5-mcrypt-5.3.17-3.38.2

php5-curl-5.3.17-3.38.2
php5-bz2-5.3.17-3.38.2
php5-snmp-5.3.17-3.38.2
php5-snmp-debuginfo-5.3.17-3.38.2
php5-sqlite-debuginfo-5.3.17-3.38.2
php5-sysvsem-debuginfo-5.3.17-3.38.2
php5-zlib-debuginfo-5.3.17-3.38.2
php5-mbstring-debuginfo-5.3.17-3.38.2
php5-bcmath-5.3.17-3.38.2
php5-soap-debuginfo-5.3.17-3.38.2
php5-gd-5.3.17-3.38.2
php5-mysql-5.3.17-3.38.2
php5-sysvshm-5.3.17-3.38.2
php5-pear-5.3.17-3.38.2
php5-dom-debuginfo-5.3.17-3.38.2
php5-json-5.3.17-3.38.2
apache2-mod_php5-debuginfo-5.3.17-3.38.2
php5-mysql-debuginfo-5.3.17-3.38.2
php5-openssl-debuginfo-5.3.17-3.38.2
php5-xmlwriter-5.3.17-3.38.2
php5-xmlrpc-debuginfo-5.3.17-3.38.2
php5-enchant-debuginfo-5.3.17-3.38.2
php5-tokenizer-debuginfo-5.3.17-3.38.2
php5-tidy-5.3.17-3.38.2
php5-pcntl-debuginfo-5.3.17-3.38.2
php5-sockets-debuginfo-5.3.17-3.38.2
php5-exif-5.3.17-3.38.2
php5-fpm-debuginfo-5.3.17-3.38.2
php5-calendar-5.3.17-3.38.2
php5-enchant-5.3.17-3.38.2
php5-odbc-5.3.17-3.38.2
php5-json-debuginfo-5.3.17-3.38.2
php5-devel-5.3.17-3.38.2
php5-ldap-5.3.17-3.38.2
php5-fastcgi-debuginfo-5.3.17-3.38.2
php5-sysvshm-debuginfo-5.3.17-3.38.2
php5-imap-5.3.17-3.38.2
php5-gettext-5.3.17-3.38.2
php5-xmlreader-debuginfo-5.3.17-3.38.2
php5-ftp-debuginfo-5.3.17-3.38.2
php5-intl-5.3.17-3.38.2
php5-curl-debuginfo-5.3.17-3.38.2
php5-readline-5.3.17-3.38.2
php5-mssql-5.3.17-3.38.2
php5-mssql-debuginfo-5.3.17-3.38.2
php5-xmlrpc-5.3.17-3.38.2
php5-suhosin-5.3.17-3.38.2
php5-gettext-debuginfo-5.3.17-3.38.2
php5-pspell-debuginfo-5.3.17-3.38.2
php5-wddx-debuginfo-5.3.17-3.38.2
php5-gd-debuginfo-5.3.17-3.38.2

142491 - SuSE SLES 11 firefox31-201411-9936 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583, CVE-2014-1585, CVE-2014-1586

Description

The scan detected that the host is missing the following update:
firefox31-201411-9936

Observation

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

https://download.suse.com/Download?buildid=eAfbLghBNgc~
https://download.suse.com/Download?buildid=7wfH0ArLzRo~
https://download.suse.com/Download?buildid=xqNNedQGCmY~

SuSE SLES 11
x86_64
mozilla-nspr-4.10.7-0.3.3
mozilla-nss-tools-3.17.2-0.3.1
mozilla-nspr-32bit-4.10.7-0.3.3
libfreebl3-3.17.2-0.3.1
MozillaFirefox-branding-SLED-31.0-0.3.1
MozillaFirefox-translations-31.2.0esr-0.9.1
mozilla-nss-3.17.2-0.3.1
MozillaFirefox-31.2.0esr-0.9.1
mozilla-nss-devel-3.17.2-0.3.1
mozilla-nss-32bit-3.17.2-0.3.1
mozilla-nspr-devel-4.10.7-0.3.3
libfreebl3-32bit-3.17.2-0.3.1

i586
mozilla-nspr-4.10.7-0.3.3
mozilla-nss-tools-3.17.2-0.3.1
libfreebl3-3.17.2-0.3.1
MozillaFirefox-branding-SLED-31.0-0.3.1
MozillaFirefox-translations-31.2.0esr-0.9.1
mozilla-nss-3.17.2-0.3.1
MozillaFirefox-31.2.0esr-0.9.1
mozilla-nss-devel-3.17.2-0.3.1
mozilla-nspr-devel-4.10.7-0.3.3

142492 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 firefox31-201411-9935 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583, CVE-2014-1585, CVE-2014-1586

Description

The scan detected that the host is missing the following update:
firefox31-201411-9935

Observation

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

https://download.suse.com/Download?buildid=Iv4PLU2TtQU~
https://download.suse.com/Download?buildid=sg4n2j3n2Y0~
https://download.suse.com/Download?buildid=22cbt5Pp3dQ~
https://download.suse.com/Download?buildid=E84BAmPyozQ~

https://download.suse.com/Download?buildid=FiQu3qRgPS8~
https://download.suse.com/Download?buildid=FPxREVnxTlU~
https://download.suse.com/Download?buildid=-e8sq6AgA24~
https://download.suse.com/Download?buildid=WZaHd9u2ym4~
https://download.suse.com/Download?buildid=-221W2D0niA~

SuSE SLED 11 SP3
x86_64
mozilla-nspr-4.10.7-0.3.3
libsoftokn3-32bit-3.17.2-0.8.1
mozilla-nspr-32bit-4.10.7-0.3.3
mozilla-nss-3.17.2-0.8.1
mozilla-nss-tools-3.17.2-0.8.1
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
MozillaFirefox-translations-31.2.0esr-0.14.2
MozillaFirefox-branding-SLED-31.0-0.8.1
libfreebl3-3.17.2-0.8.1
mozilla-nss-32bit-3.17.2-0.8.1
libfreebl3-32bit-3.17.2-0.8.1

i586
mozilla-nspr-4.10.7-0.3.3
libfreebl3-3.17.2-0.8.1
mozilla-nss-3.17.2-0.8.1
mozilla-nss-tools-3.17.2-0.8.1
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
MozillaFirefox-translations-31.2.0esr-0.14.2
MozillaFirefox-branding-SLED-31.0-0.8.1

SuSE SLES 11 SP3
x86_64
mozilla-nspr-4.10.7-0.3.3
libsoftokn3-32bit-3.17.2-0.8.1
mozilla-nspr-32bit-4.10.7-0.3.3
mozilla-nss-3.17.2-0.8.1
mozilla-nss-tools-3.17.2-0.8.1
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
MozillaFirefox-translations-31.2.0esr-0.14.2
MozillaFirefox-branding-SLED-31.0-0.8.1
libfreebl3-3.17.2-0.8.1
mozilla-nss-32bit-3.17.2-0.8.1
libfreebl3-32bit-3.17.2-0.8.1

i586
mozilla-nspr-4.10.7-0.3.3
libfreebl3-3.17.2-0.8.1
mozilla-nss-3.17.2-0.8.1
mozilla-nss-tools-3.17.2-0.8.1
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
MozillaFirefox-translations-31.2.0esr-0.14.2
MozillaFirefox-branding-SLED-31.0-0.8.1

SuSE SLED 11
x86_64
libsoftokn3-32bit-3.17.2-0.8.1
MozillaFirefox-branding-SLES-for-VMware-31.0-0.3.1

mozilla-nspr-32bit-4.10.7-0.3.3
mozilla-nss-3.17.2-0.8.1
mozilla-nspr-4.10.7-0.3.3
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
mozilla-nss-tools-3.17.2-0.8.1
MozillaFirefox-translations-31.2.0esr-0.14.2
mozilla-nss-32bit-3.17.2-0.8.1
libfreebl3-3.17.2-0.8.1
libfreebl3-32bit-3.17.2-0.8.1

i586
mozilla-nspr-4.10.7-0.3.3
MozillaFirefox-branding-SLES-for-VMware-31.0-0.3.1
mozilla-nss-3.17.2-0.8.1
mozilla-nss-tools-3.17.2-0.8.1
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
MozillaFirefox-translations-31.2.0esr-0.14.2
libfreebl3-3.17.2-0.8.1

SuSE SLES 11
x86_64
libsoftokn3-32bit-3.17.2-0.8.1
MozillaFirefox-branding-SLES-for-VMware-31.0-0.3.1
mozilla-nspr-32bit-4.10.7-0.3.3
mozilla-nss-3.17.2-0.8.1
mozilla-nspr-4.10.7-0.3.3
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
mozilla-nss-tools-3.17.2-0.8.1
MozillaFirefox-translations-31.2.0esr-0.14.2
mozilla-nss-32bit-3.17.2-0.8.1
libfreebl3-3.17.2-0.8.1
libfreebl3-32bit-3.17.2-0.8.1

i586
mozilla-nspr-4.10.7-0.3.3
MozillaFirefox-branding-SLES-for-VMware-31.0-0.3.1
mozilla-nss-3.17.2-0.8.1
mozilla-nss-tools-3.17.2-0.8.1
libsoftokn3-3.17.2-0.8.1
MozillaFirefox-31.2.0esr-0.14.2
MozillaFirefox-translations-31.2.0esr-0.14.2
libfreebl3-3.17.2-0.8.1

142493 - SuSE SLES 10, 10 SP4 openssl-8982 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Description

The scan detected that the host is missing the following update:
openssl-8982

Observation

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

For more information see:

https://download.suse.com/Download?buildid=9t9gBLla3Mc~
https://download.suse.com/Download?buildid=n3ant0zj5Tc~
https://download.suse.com/Download?buildid=sDIBAM7sAuo~
https://download.suse.com/Download?buildid=nUc_X2ci6Wg~
https://download.suse.com/Download?buildid=q0X955amn2E~
https://download.suse.com/Download?buildid=hAU1owYph28~

SuSE SLES 10
x86_64
openssl-devel-0.9.8a-18.86.3
openssl-0.9.8a-18.86.3
openssl-32bit-0.9.8a-18.86.3
openssl-devel-32bit-0.9.8a-18.86.3
openssl-doc-0.9.8a-18.86.3

i586
openssl-devel-0.9.8a-18.86.3
openssl-0.9.8a-18.86.3
openssl-doc-0.9.8a-18.86.3

SuSE SLES 10 SP4
x86_64
openssl-debuginfo-0.9.8a-18.86.3

i586
openssl-debuginfo-0.9.8a-18.86.3

142494 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 libopenssl-devel-9915 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Description

The scan detected that the host is missing the following update:
libopenssl-devel-9915

Observation

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

https://download.suse.com/Download?buildid=ywMv5mwKhnA~
https://download.suse.com/Download?buildid=Yvmk80Tkwq4~
https://download.suse.com/Download?buildid=4x8FpBlf_Zk~
https://download.suse.com/Download?buildid=omF73c8QLOY~
https://download.suse.com/Download?buildid=txPQ-AHBi-k~
https://download.suse.com/Download?buildid=Xjh3YyVtzLk~
https://download.suse.com/Download?buildid=rWh-lSsKFiE~
https://download.suse.com/Download?buildid=GvWKcgwhrgo~
https://download.suse.com/Download?buildid=91r44HTebRc~

SuSE SLED 11 SP3
x86_64
openssl-0.9.8j-0.66.1
libopenssl0_9_8-32bit-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

i586
openssl-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

SuSE SLES 11 SP3
x86_64
libopenssl0_9_8-hmac-32bit-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-doc-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-32bit-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

i586
openssl-doc-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

SuSE SLED 11
x86_64
libopenssl0_9_8-hmac-32bit-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-doc-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-32bit-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

i586
openssl-doc-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

SuSE SLES 11
x86_64
libopenssl0_9_8-hmac-32bit-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-doc-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-32bit-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

i586
openssl-doc-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

142498 - SuSE SLES 11 libopenssl-devel-9928 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Description

The scan detected that the host is missing the following update:
libopenssl-devel-9928

Observation

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

https://download.suse.com/Download?buildid=lvLvN5TO3sQ~
https://download.suse.com/Download?buildid=b4kpzOpNr0E~
https://download.suse.com/Download?buildid=ML3SWY9woYg~

SuSE SLES 11
x86_64
libopenssl0_9_8-hmac-32bit-0.9.8j-0.66.1
libopenssl-devel-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-doc-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-32bit-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

i586
openssl-doc-0.9.8j-0.66.1
libopenssl-devel-0.9.8j-0.66.1
libopenssl0_9_8-hmac-0.9.8j-0.66.1
openssl-0.9.8j-0.66.1
libopenssl0_9_8-0.9.8j-0.66.1

170416 - Amazon Linux AMI ALAS-2014-436 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4002

Description

The scan detected that the host is missing the following update:
ALAS-2014-436

Observation

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

https://alas.aws.amazon.com/ALAS-2014-436.html

Amazon Linux AMI
noarch
xerces-j2-scripts-2.7.1-12.7.19.amzn1
xerces-j2-2.7.1-12.7.19.amzn1
xerces-j2-javadoc-apis-2.7.1-12.7.19.amzn1
xerces-j2-demo-2.7.1-12.7.19.amzn1
xerces-j2-javadoc-xni-2.7.1-12.7.19.amzn1
xerces-j2-javadoc-other-2.7.1-12.7.19.amzn1
xerces-j2-javadoc-impl-2.7.1-12.7.19.amzn1

170417 - Amazon Linux AMI ALAS-2014-435 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
ALAS-2014-435

Observation

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

https://alas.aws.amazon.com/ALAS-2014-435.html

Amazon Linux AMI
x86_64
php55-process-5.5.18-1.92.amzn1
php55-mssql-5.5.18-1.92.amzn1
php55-pspell-5.5.18-1.92.amzn1
php55-mcrypt-5.5.18-1.92.amzn1
php55-enchant-5.5.18-1.92.amzn1
php55-common-5.5.18-1.92.amzn1
php55-ldap-5.5.18-1.92.amzn1
php55-xml-5.5.18-1.92.amzn1
php55-debuginfo-5.5.18-1.92.amzn1
php55-cli-5.5.18-1.92.amzn1
php55-mysqlnd-5.5.18-1.92.amzn1
php55-tidy-5.5.18-1.92.amzn1
php55-snmp-5.5.18-1.92.amzn1
php55-odbc-5.5.18-1.92.amzn1
php55-pdo-5.5.18-1.92.amzn1
php55-gmp-5.5.18-1.92.amzn1
php55-gd-5.5.18-1.92.amzn1
php55-mbstring-5.5.18-1.92.amzn1
php55-devel-5.5.18-1.92.amzn1
php55-bcmath-5.5.18-1.92.amzn1
php55-dba-5.5.18-1.92.amzn1
php55-imap-5.5.18-1.92.amzn1
php55-pgsql-5.5.18-1.92.amzn1
php55-soap-5.5.18-1.92.amzn1
php55-intl-5.5.18-1.92.amzn1
php55-xmlrpc-5.5.18-1.92.amzn1
php55-fpm-5.5.18-1.92.amzn1
php55-opcache-5.5.18-1.92.amzn1
php55-embedded-5.5.18-1.92.amzn1
php55-recode-5.5.18-1.92.amzn1
php55-5.5.18-1.92.amzn1

i686
php55-process-5.5.18-1.92.amzn1
php55-pspell-5.5.18-1.92.amzn1
php55-enchant-5.5.18-1.92.amzn1
php55-xml-5.5.18-1.92.amzn1
php55-mssql-5.5.18-1.92.amzn1
php55-common-5.5.18-1.92.amzn1
php55-ldap-5.5.18-1.92.amzn1
php55-embedded-5.5.18-1.92.amzn1
php55-debuginfo-5.5.18-1.92.amzn1
php55-cli-5.5.18-1.92.amzn1
php55-mysqlnd-5.5.18-1.92.amzn1
php55-mcrypt-5.5.18-1.92.amzn1
php55-snmp-5.5.18-1.92.amzn1
php55-odbc-5.5.18-1.92.amzn1

php55-pdo-5.5.18-1.92.amzn1
php55-intl-5.5.18-1.92.amzn1
php55-gmp-5.5.18-1.92.amzn1
php55-gd-5.5.18-1.92.amzn1
php55-mbstring-5.5.18-1.92.amzn1
php55-devel-5.5.18-1.92.amzn1
php55-bcmath-5.5.18-1.92.amzn1
php55-dba-5.5.18-1.92.amzn1
php55-pgsql-5.5.18-1.92.amzn1
php55-soap-5.5.18-1.92.amzn1
php55-imap-5.5.18-1.92.amzn1
php55-tidy-5.5.18-1.92.amzn1
php55-xmlrpc-5.5.18-1.92.amzn1
php55-fpm-5.5.18-1.92.amzn1
php55-opcache-5.5.18-1.92.amzn1
php55-recode-5.5.18-1.92.amzn1
php55-5.5.18-1.92.amzn1

170418 - Amazon Linux AMI ALAS-2014-434 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
ALAS-2014-434

Observation

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

https://alas.aws.amazon.com/ALAS-2014-434.html

Amazon Linux AMI
x86_64
php54-mssql-5.4.34-1.62.amzn1
php54-mbstring-5.4.34-1.62.amzn1
php54-mcrypt-5.4.34-1.62.amzn1
php54-odbc-5.4.34-1.62.amzn1
php54-soap-5.4.34-1.62.amzn1
php54-devel-5.4.34-1.62.amzn1
php54-recode-5.4.34-1.62.amzn1
php54-xmlrpc-5.4.34-1.62.amzn1
php54-fpm-5.4.34-1.62.amzn1
php54-gd-5.4.34-1.62.amzn1
php54-dba-5.4.34-1.62.amzn1
php54-xml-5.4.34-1.62.amzn1
php54-pgsql-5.4.34-1.62.amzn1
php54-pdo-5.4.34-1.62.amzn1
php54-process-5.4.34-1.62.amzn1
php54-5.4.34-1.62.amzn1
php54-tidy-5.4.34-1.62.amzn1
php54-ldap-5.4.34-1.62.amzn1
php54-embedded-5.4.34-1.62.amzn1
php54-enchant-5.4.34-1.62.amzn1
php54-cli-5.4.34-1.62.amzn1
php54-common-5.4.34-1.62.amzn1

php54-imap-5.4.34-1.62.amzn1
php54-intl-5.4.34-1.62.amzn1
php54-bcmath-5.4.34-1.62.amzn1
php54-mysqlnd-5.4.34-1.62.amzn1
php54-mysql-5.4.34-1.62.amzn1
php54-snmp-5.4.34-1.62.amzn1
php54-pspell-5.4.34-1.62.amzn1
php54-debuginfo-5.4.34-1.62.amzn1

i686
php54-xmlrpc-5.4.34-1.62.amzn1
php54-mbstring-5.4.34-1.62.amzn1
php54-process-5.4.34-1.62.amzn1
php54-mcrypt-5.4.34-1.62.amzn1
php54-odbc-5.4.34-1.62.amzn1
php54-ldap-5.4.34-1.62.amzn1
php54-soap-5.4.34-1.62.amzn1
php54-tidy-5.4.34-1.62.amzn1
php54-recode-5.4.34-1.62.amzn1
php54-5.4.34-1.62.amzn1
php54-fpm-5.4.34-1.62.amzn1
php54-gd-5.4.34-1.62.amzn1
php54-dba-5.4.34-1.62.amzn1
php54-pgsql-5.4.34-1.62.amzn1
php54-pdo-5.4.34-1.62.amzn1
php54-pspell-5.4.34-1.62.amzn1
php54-intl-5.4.34-1.62.amzn1
php54-embedded-5.4.34-1.62.amzn1
php54-devel-5.4.34-1.62.amzn1
php54-xml-5.4.34-1.62.amzn1
php54-enchant-5.4.34-1.62.amzn1
php54-mssql-5.4.34-1.62.amzn1
php54-cli-5.4.34-1.62.amzn1
php54-common-5.4.34-1.62.amzn1
php54-imap-5.4.34-1.62.amzn1
php54-bcmath-5.4.34-1.62.amzn1
php54-mysqlnd-5.4.34-1.62.amzn1
php54-mysql-5.4.34-1.62.amzn1
php54-snmp-5.4.34-1.62.amzn1
php54-debuginfo-5.4.34-1.62.amzn1

174586 - Scientific Linux Security ERRATA Important: php on SL5.x i386/x86_64 (1411-2298)

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

Risk Level: High

CVE: CVE-2014-3669, CVE-2014-3670, CVE-2014-8626

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: php on SL5.x i386/x86_64 (1411-2298)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=2298

SL5

x86_64
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-debuginfo-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

i386
php-cli-5.1.6-45.el5_11
php-dba-5.1.6-45.el5_11
php-ldap-5.1.6-45.el5_11
php-5.1.6-45.el5_11
php-xml-5.1.6-45.el5_11
php-debuginfo-5.1.6-45.el5_11
php-xmlrpc-5.1.6-45.el5_11
php-soap-5.1.6-45.el5_11
php-mbstring-5.1.6-45.el5_11
php-odbc-5.1.6-45.el5_11
php-common-5.1.6-45.el5_11
php-pdo-5.1.6-45.el5_11
php-mysql-5.1.6-45.el5_11
php-imap-5.1.6-45.el5_11
php-snmp-5.1.6-45.el5_11
php-gd-5.1.6-45.el5_11
php-devel-5.1.6-45.el5_11
php-ncurses-5.1.6-45.el5_11
php-bcmath-5.1.6-45.el5_11
php-pgsql-5.1.6-45.el5_11

174587 - Scientific Linux Security ERRATA Important: mod_auth_mellon on SL6.x i386/x86_64 (1411-2421)

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

Risk Level: High

CVE: CVE-2014-8566, CVE-2014-8567

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: mod_auth_mellon on SL6.x i386/x86_64 (1411-2421)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=2421

SL6
x86_64
mod_auth_mellon-debuginfo-0.8.0-3.el6_6
mod_auth_mellon-0.8.0-3.el6_6

i386
mod_auth_mellon-debuginfo-0.8.0-3.el6_6
mod_auth_mellon-0.8.0-3.el6_6

177988 - Gentoo Linux GLSA-201411-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
GLSA-201411-04

Observation

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

http://security.gentoo.org/glsa/glsa-201411-04.xml

Affected packages:
dev-lang/php < 5.5.18

184605 - Ubuntu Linux 14.04, 14.10 USN-2398-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3693

Description

The scan detected that the host is missing the following update:
USN-2398-1

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-November/002716.html

Ubuntu 14.10

libreoffice-core_4.3.3-0ubuntu1

Ubuntu 14.04

libreoffice-core_4.2.7-0ubuntu1

188428 - Fedora Linux 21 FEDORA-2014-12934 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-2014-12934

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142614.html

Fedora Core 21

drupal7-7.32-1.fc21

188429 - Fedora Linux 20 FEDORA-2014-13574 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8350

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13574

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142696.html

Fedora Core 20

php-Smarty-3.1.21-1.fc20

188431 - Fedora Linux 21 FEDORA-2014-12875 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12875

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141872.html

Fedora Core 21

sysklogd-1.5-18.fc21

188432 - Fedora Linux 19 FEDORA-2014-13570 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8350

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13570

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142687.html

Fedora Core 19

php-Smarty-3.1.21-1.fc19

188445 - Fedora Linux 21 FEDORA-2014-13581 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3675, CVE-2014-3676, CVE-2014-3677

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13581

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142496.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142497.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142495.html

Fedora Core 21

shim-signed-0.8-1.fc22
mokutil-0.2.0-1.fc21
shim-0.8-1.fc22

188464 - Fedora Linux 21 FEDORA-2014-13618 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8350

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13618

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143123.html

Fedora Core 21

php-Smarty-3.1.21-1.fc21

188483 - Fedora Linux 21 FEDORA-2014-12983 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12983

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142132.html

Fedora Core 21

php-5.6.2-1.fc21

188485 - Fedora Linux 21 FEDORA-2014-14126 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3610, CVE-2014-3611, CVE-2014-3646, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-8369, CVE-2014-8480, CVE-2014-8481

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14126

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142663.html

Fedora Core 21

kernel-3.17.2-300.fc21

17342 - (SOL15680) F5 BIG-IP Multiple Linux Kernel Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-0205, CVE-2014-3535, CVE-2014-3917, CVE-2014-4667

Description

Multiple denial of service 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 denial of service vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition.

17348 - McAfee Endpoint EEFF/FRP Insufficient Entropy Information Disclosure

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

Risk Level: Medium

CVE: CVE-2014-8518

Description

A vulnerability in some versions of McAfee Endpoint Encryption for Files and Folders and McAfee File and Removable Media Protection could lead to information disclosure.

Observation

A vulnerability in some versions of McAfee Endpoint Encryption for Files and Folders and McAfee File and Removable Media Protection could lead to information disclosure.

The flaw lies in the removable media or CD and DVD encryption offsite access options. Successful exploitation by a local attacker could result in the disclosure of sensitive information.

85823 - CentOS 6 CESA-2014-1843 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3185, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646

Description

The scan detected that the host is missing the following update:
CESA-2014-1843

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020748.html

CentOS 6
x86_64
kernel-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6

perf-2.6.32-504.1.3.el6
python-perf-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6

i686
kernel-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6
python-perf-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6

noarch
kernel-doc-2.6.32-504.1.3.el6
kernel-firmware-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6

91656 - Oracle Enterprise Linux ELSA-2014-1843 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3185, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646

Description

The scan detected that the host is missing the following update:
ELSA-2014-1843

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004630.html

OEL6
x86_64
kernel-firmware-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6
kernel-doc-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
python-perf-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6

i386
kernel-firmware-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6
kernel-doc-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
python-perf-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6

perf-2.6.32-504.1.3.el6

91659 - Oracle Enterprise Linux ELSA-2014-1827 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6055

Description

The scan detected that the host is missing the following update:
ELSA-2014-1827

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004628.html

OEL7
x86_64
kdenetwork-4.10.5-8.el7_0
kdenetwork-common-4.10.5-8.el7_0
kdenetwork-kopete-libs-4.10.5-8.el7_0
kdenetwork-krfb-4.10.5-8.el7_0
kdenetwork-krdc-devel-4.10.5-8.el7_0
kdenetwork-devel-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0
kdenetwork-kopete-devel-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-kdnssd-4.10.5-8.el7_0
kdenetwork-fileshare-samba-4.10.5-8.el7_0
kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-kopete-4.10.5-8.el7_0
kdenetwork-krdc-4.10.5-8.el7_0
kdenetwork-kget-4.10.5-8.el7_0

140603 - Red Hat Enterprise Linux RHSA-2014-1827 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
RHSA-2014-1827

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1827.html

RHEL7WS
x86_64
kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-kopete-4.10.5-8.el7_0

kdenetwork-kopete-libs-4.10.5-8.el7_0
kdenetwork-krfb-4.10.5-8.el7_0
kdenetwork-krdc-devel-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0
kdenetwork-kopete-devel-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-kdnssd-4.10.5-8.el7_0
kdenetwork-debuginfo-4.10.5-8.el7_0
kdenetwork-krdc-4.10.5-8.el7_0
kdenetwork-kget-4.10.5-8.el7_0

noarch
kdenetwork-devel-4.10.5-8.el7_0
kdenetwork-common-4.10.5-8.el7_0

RHEL7D
x86_64
kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-krfb-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0
kdenetwork-kdnssd-4.10.5-8.el7_0
kdenetwork-debuginfo-4.10.5-8.el7_0
kdenetwork-krdc-4.10.5-8.el7_0
kdenetwork-kget-4.10.5-8.el7_0

noarch
kdenetwork-common-4.10.5-8.el7_0

RHEL7S
x86_64
kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-kopete-4.10.5-8.el7_0
kdenetwork-kopete-libs-4.10.5-8.el7_0
kdenetwork-krfb-4.10.5-8.el7_0
kdenetwork-krdc-devel-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0
kdenetwork-kopete-devel-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-kdnssd-4.10.5-8.el7_0
kdenetwork-debuginfo-4.10.5-8.el7_0
kdenetwork-krdc-4.10.5-8.el7_0
kdenetwork-kget-4.10.5-8.el7_0

noarch
kdenetwork-devel-4.10.5-8.el7_0
kdenetwork-common-4.10.5-8.el7_0

140605 - Red Hat Enterprise Linux RHSA-2014-1843 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3185, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646

Description

The scan detected that the host is missing the following update:
RHSA-2014-1843

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1843.html

RHEL6D
x86_64
kernel-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6

i386
kernel-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6
kernel-debuginfo-common-i686-2.6.32-504.1.3.el6

noarch
kernel-doc-2.6.32-504.1.3.el6
kernel-firmware-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6

RHEL6S
x86_64
kernel-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6

i386
kernel-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6

perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6
kernel-debuginfo-common-i686-2.6.32-504.1.3.el6

noarch
kernel-doc-2.6.32-504.1.3.el6
kernel-firmware-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6

RHEL6WS
x86_64
kernel-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6

i386
kernel-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6
kernel-debuginfo-common-i686-2.6.32-504.1.3.el6

noarch
kernel-doc-2.6.32-504.1.3.el6
kernel-firmware-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6

142486 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 wpa_supplicant-9894 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:
wpa_supplicant-9894

Observation

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

https://download.suse.com/Download?buildid=xeyQLMAsN2A~
https://download.suse.com/Download?buildid=bKD75THQFqs~

https://download.suse.com/Download?buildid=igxPoc9nZ2I~
https://download.suse.com/Download?buildid=Zh7gI0FyrqM~
https://download.suse.com/Download?buildid=UzsFDrL3XM0~
https://download.suse.com/Download?buildid=ZoqA72FcOt4~
https://download.suse.com/Download?buildid=jMZpoMjkEno~
https://download.suse.com/Download?buildid=gFhiHxSbIqg~
https://download.suse.com/Download?buildid=_X961RwyE9U~

SuSE SLED 11 SP3
x86_64
wpa_supplicant-0.7.1-6.15.1
wpa_supplicant-gui-0.7.1-6.15.1

i586
wpa_supplicant-0.7.1-6.15.1
wpa_supplicant-gui-0.7.1-6.15.1

SuSE SLES 11 SP3
x86_64
wpa_supplicant-0.7.1-6.15.1

i586
wpa_supplicant-0.7.1-6.15.1

SuSE SLED 11
x86_64
wpa_supplicant-0.7.1-6.15.1

i586
wpa_supplicant-0.7.1-6.15.1

SuSE SLES 11
x86_64
wpa_supplicant-0.7.1-6.15.1

i586
wpa_supplicant-0.7.1-6.15.1

142490 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1376-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
openSUSE-SU-2014:1376-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00023.html

SuSE Linux 13.1
i586
libpurple-tcl-debuginfo-2.10.10-4.22.1
libpurple-debuginfo-2.10.10-4.22.1

libpurple-lang-2.10.10-4.22.1
finch-devel-2.10.10-4.22.1
pidgin-2.10.10-4.22.1
pidgin-debuginfo-2.10.10-4.22.1
libpurple-branding-openSUSE-13.1-2.17.1
pidgin-otr-debugsource-4.0.0-4.7.1
libpurple-devel-2.10.10-4.22.1
finch-2.10.10-4.22.1
finch-debuginfo-2.10.10-4.22.1
libpurple-tcl-2.10.10-4.22.1
pidgin-otr-debuginfo-4.0.0-4.7.1
libpurple-2.10.10-4.22.1
libpurple-meanwhile-debuginfo-2.10.10-4.22.1
pidgin-devel-2.10.10-4.22.1
libpurple-meanwhile-2.10.10-4.22.1
pidgin-otr-4.0.0-4.7.1
libpurple-branding-upstream-2.10.10-4.22.1
pidgin-debugsource-2.10.10-4.22.1

SuSE Linux 12.3
i586
pidgin-devel-2.10.10-4.16.1
pidgin-otr-debuginfo-4.0.0-2.11.1
libpurple-2.10.10-4.16.1
libpurple-debuginfo-2.10.10-4.16.1
pidgin-debugsource-2.10.10-4.16.1
pidgin-otr-debugsource-4.0.0-2.11.1
pidgin-2.10.10-4.16.1
libpurple-branding-upstream-2.10.10-4.16.1
libpurple-devel-2.10.10-4.16.1
finch-2.10.10-4.16.1
finch-debuginfo-2.10.10-4.16.1
libpurple-tcl-debuginfo-2.10.10-4.16.1
libpurple-meanwhile-2.10.10-4.16.1
finch-devel-2.10.10-4.16.1
libpurple-meanwhile-debuginfo-2.10.10-4.16.1
libpurple-branding-openSUSE-12.2-4.21.1
pidgin-otr-4.0.0-2.11.1
pidgin-debuginfo-2.10.10-4.16.1
libpurple-tcl-2.10.10-4.16.1
libpurple-lang-2.10.10-4.16.1

188425 - Fedora Linux 19 FEDORA-2014-13778 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13778

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142770.html

Fedora Core 19

hostapd-2.0-5.fc19

188426 - Fedora Linux 21 FEDORA-2014-14112 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora 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:
FEDORA-2014-14112

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143147.html

Fedora Core 21

pidgin-2.10.10-2.fc21

188434 - Fedora Linux 21 FEDORA-2014-13537 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13537

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143100.html

Fedora Core 21

wpa_supplicant-2.0-12.fc21

188439 - Fedora Linux 20 FEDORA-2014-13783 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13783

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142830.html

Fedora Core 20

hostapd-2.3-1.fc20

188452 - Fedora Linux 21 FEDORA-2014-13608 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13608

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141865.html

Fedora Core 21

hostapd-2.3-1.fc21

188489 - Fedora Linux 20 FEDORA-2014-14069 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora 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:
FEDORA-2014-14069

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143310.html

Fedora Core 20

pidgin-2.10.10-1.fc20

17220 - Cisco Adaptive Security Appliance Software RAMFS Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3399

Description

A vulnerability in some versions of Cisco Adaptive Security Appliance Software could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco Adaptive Security Appliance Software could lead to a denial of service.

The flaw lies in the SSL VPN implementation. Successful exploitation by a remote attacker could result in a denial of service condition.

17326 - MariaDB Multiple Vulnerabilities Prior To 5.5.40

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

Risk Level: Medium

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 MariaDB.

Observation

MariaDB is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of MariaDB. The flaws are due to errors in multiple components. Successful exploitation could allow an attacker to disclose potentially sensitive information, manipulate certain data, cause a Denial of Service, and compromise a vulnerable system.

17346 - Cisco IOS Ethernet Connectivity Fault Management Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3409

Description

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

Observation

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

The flaw lies in the Ethernet Connectivity Fault Management feature. Successful exploitation by a remote attacker could result in a denial of service condition.

17351 - WordPress Cart66-Lite Plugin Cross Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5977

Description

A Cross-site request forgery vulnerability is present in some versions of Cart66 Lite Plugin for WordPress.

Observation

WordPress is a popular blog web application.

A Cross-site request forgery vulnerability is present in some versions of Cart66 Lite Plugin for WordPress. The flaw lies in Cart66Product.php. Successful exploitation could allow an attacker to execute remote code.

17352 - MariaDB Multiple Vulnerabilities Prior To 5.5.37

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

Risk Level: Medium

CVE: CVE-2014-0384, CVE-2014-2419, CVE-2014-2430, CVE-2014-2431, CVE-2014-2432, CVE-2014-2436, CVE-2014-2438, CVE-2014-2440

Description

Multiple vulnerabilities are present in some versions of MariaDB.

Observation

MariaDB is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of MariaDB. The flaws are due to errors in multiple components. Successful exploitation could allow an attacker to disclose potentially sensitive information, manipulate certain data, or cause a denial of service.

58990 - Debian Linux 7.0 DSA-3070-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3711, CVE-2014-3952, CVE-2014-3953, CVE-2014-8476

Description

The scan detected that the host is missing the following update:
DSA-3070-1

Observation

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

http://www.debian.org/security/2014/dsa-3070

Debian 7.0
all
kfreebsd-headers-9.0-2-xen_9.0-10+deb70.8
crypto-modules-9.0-2-486-di_9.0-10+deb70.8
nfs-modules-9.0-2-486-di_9.0-10+deb70.8
nic-wireless-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-headers-9-686-smp_9.0-10+deb70.8
nic-modules-9.0-2-amd64-di_9.0-10+deb70.8
serial-modules-9.0-2-amd64-di_9.0-10+deb70.8
plip-modules-9.0-2-amd64-di_9.0-10+deb70.8
zlib-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-headers-9-amd64_9.0-10+deb70.8
kernel-image-9.0-2-amd64-di_9.0-10+deb70.8
i2c-modules-9.0-2-486-di_9.0-10+deb70.8
crypto-dm-modules-9.0-2-amd64-di_9.0-10+deb70.8
nullfs-modules-9.0-2-amd64-di_9.0-10+deb70.8
cdrom-modules-9.0-2-amd64-di_9.0-10+deb70.8

scsi-core-modules-9.0-2-486-di_9.0-10+deb70.8
parport-modules-9.0-2-486-di_9.0-10+deb70.8
sound-modules-9.0-2-amd64-di_9.0-10+deb70.8
fat-modules-9.0-2-amd64-di_9.0-10+deb70.8
ext2-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9.0-2-686_9.0-10+deb70.8
nullfs-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-image-9.0-2-486_9.0-10+deb70.8
kfreebsd-headers-9-486_9.0-10+deb70.8
mmc-core-modules-9.0-2-amd64-di_9.0-10+deb70.8
ipv6-modules-9.0-2-amd64-di_9.0-10+deb70.8
nic-wireless-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9-xen_9.0-10+deb70.8
cdrom-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-image-9-malta_9.0-10+deb70.8
kfreebsd-image-9-xen_9.0-10+deb70.8
zfs-modules-9.0-2-486-di_9.0-10+deb70.8
acpi-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-image-9-486_9.0-10+deb70.8
kfreebsd-image-9-686-smp_9.0-10+deb70.8
ntfs-modules-9.0-2-486-di_9.0-10+deb70.8
xfs-modules-9.0-2-amd64-di_9.0-10+deb70.8
nic-shared-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-image-9.0-2-amd64_9.0-10+deb70.8
ppp-modules-9.0-2-amd64-di_9.0-10+deb70.8
scsi-core-modules-9.0-2-amd64-di_9.0-10+deb70.8
ppp-modules-9.0-2-486-di_9.0-10+deb70.8
nfs-modules-9.0-2-amd64-di_9.0-10+deb70.8
serial-modules-9.0-2-486-di_9.0-10+deb70.8
zfs-modules-9.0-2-amd64-di_9.0-10+deb70.8
kernel-image-9.0-2-486-di_9.0-10+deb70.8
ext2-modules-9.0-2-amd64-di_9.0-10+deb70.8
crypto-dm-modules-9.0-2-486-di_9.0-10+deb70.8
scsi-extra-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-source-9.0_9.0-10+deb70.8
parport-modules-9.0-2-amd64-di_9.0-10+deb70.8
mmc-modules-9.0-2-amd64-di_9.0-10+deb70.8
md-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-headers-9.0-2-malta_9.0-10+deb70.8
mmc-core-modules-9.0-2-486-di_9.0-10+deb70.8
plip-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9.0-2-486_9.0-10+deb70.8
kfreebsd-image-9.0-2-686_9.0-10+deb70.8
reiserfs-modules-9.0-2-amd64-di_9.0-10+deb70.8
ipv6-modules-9.0-2-486-di_9.0-10+deb70.8
isofs-modules-9.0-2-486-di_9.0-10+deb70.8
nic-modules-9.0-2-486-di_9.0-10+deb70.8
sound-modules-9.0-2-486-di_9.0-10+deb70.8
loop-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-image-9.0-2-malta_9.0-10+deb70.8
kfreebsd-headers-9.0-2_9.0-10+deb70.8
sata-modules-9.0-2-486-di_9.0-10+deb70.8
xfs-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9-686_9.0-10+deb70.8
floppy-modules-9.0-2-486-di_9.0-10+deb70.8
zlib-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9-malta_9.0-10+deb70.8
ntfs-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-image-9-amd64_9.0-10+deb70.8
scsi-extra-modules-9.0-2-amd64-di_9.0-10+deb70.8

kfreebsd-image-9.0-2-xen_9.0-10+deb70.8
floppy-modules-9.0-2-amd64-di_9.0-10+deb70.8
i2c-modules-9.0-2-amd64-di_9.0-10+deb70.8
acpi-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9.0-2-amd64_9.0-10+deb70.8
nic-shared-modules-9.0-2-amd64-di_9.0-10+deb70.8
sata-modules-9.0-2-amd64-di_9.0-10+deb70.8
isofs-modules-9.0-2-amd64-di_9.0-10+deb70.8
kfreebsd-image-9.0-2-686-smp_9.0-10+deb70.8
fat-modules-9.0-2-486-di_9.0-10+deb70.8
nls-core-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-image-9-686_9.0-10+deb70.8
mmc-modules-9.0-2-486-di_9.0-10+deb70.8
loop-modules-9.0-2-486-di_9.0-10+deb70.8
crypto-modules-9.0-2-amd64-di_9.0-10+deb70.8
scsi-modules-9.0-2-486-di_9.0-10+deb70.8
kfreebsd-headers-9.0-2-686-smp_9.0-10+deb70.8
reiserfs-modules-9.0-2-486-di_9.0-10+deb70.8
md-modules-9.0-2-486-di_9.0-10+deb70.8
scsi-modules-9.0-2-amd64-di_9.0-10+deb70.8
nls-core-modules-9.0-2-amd64-di_9.0-10+deb70.8

58994 - Debian Linux 7.0 DSA-3068-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
DSA-3068-1

Observation

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

http://www.debian.org/security/2014/dsa-3068

Debian 7.0
all
konversation_1.4-1+deb7u1

142496 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1382-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1382-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00028.html

SuSE Linux 13.1
i586
quassel-mono-0.9.2-16.1
quassel-core-0.9.2-16.1
quassel-client-debuginfo-0.9.2-16.1
quassel-base-0.9.2-16.1
quassel-mono-debuginfo-0.9.2-16.1
quassel-client-0.9.2-16.1
quassel-debugsource-0.9.2-16.1
quassel-core-debuginfo-0.9.2-16.1

SuSE Linux 12.3
i586
quassel-client-0.8.0-5.4.1
quassel-base-0.8.0-5.4.1
quassel-core-0.8.0-5.4.1
quassel-mono-0.8.0-5.4.1
quassel-client-debuginfo-0.8.0-5.4.1
quassel-mono-debuginfo-0.8.0-5.4.1
quassel-debugsource-0.8.0-5.4.1
quassel-core-debuginfo-0.8.0-5.4.1

SuSE Linux 13.2
i586
quassel-core-0.10.0-3.4.1
quassel-core-debuginfo-0.10.0-3.4.1
quassel-mono-0.10.0-3.4.1
quassel-mono-debuginfo-0.10.0-3.4.1
quassel-client-debuginfo-0.10.0-3.4.1
quassel-client-0.10.0-3.4.1
quassel-debugsource-0.10.0-3.4.1
quassel-base-0.10.0-3.4.1

170412 - Amazon Linux AMI ALAS-2014-439 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8080

Description

The scan detected that the host is missing the following update:
ALAS-2014-439

Observation

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

https://alas.aws.amazon.com/ALAS-2014-439.html

Amazon Linux AMI
x86_64
ruby21-debuginfo-2.1.4-1.14.amzn1
rubygem21-bigdecimal-1.2.4-1.14.amzn1
ruby21-devel-2.1.4-1.14.amzn1
rubygem21-io-console-0.4.2-1.14.amzn1
ruby21-libs-2.1.4-1.14.amzn1

ruby21-2.1.4-1.14.amzn1
rubygem21-psych-2.0.5-1.14.amzn1

i686
rubygem21-bigdecimal-1.2.4-1.14.amzn1
ruby21-debuginfo-2.1.4-1.14.amzn1
rubygem21-io-console-0.4.2-1.14.amzn1
ruby21-libs-2.1.4-1.14.amzn1
ruby21-2.1.4-1.14.amzn1
rubygem21-psych-2.0.5-1.14.amzn1
ruby21-devel-2.1.4-1.14.amzn1

noarch
rubygems21-devel-2.2.2-1.14.amzn1
ruby21-doc-2.1.4-1.14.amzn1
ruby21-irb-2.1.4-1.14.amzn1
rubygems21-2.2.2-1.14.amzn1

170414 - Amazon Linux AMI ALAS-2014-441 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8080

Description

The scan detected that the host is missing the following update:
ALAS-2014-441

Observation

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

https://alas.aws.amazon.com/ALAS-2014-441.html

Amazon Linux AMI
x86_64
rubygem20-bigdecimal-1.2.0-1.19.amzn1
ruby20-2.0.0.594-1.19.amzn1
ruby20-devel-2.0.0.594-1.19.amzn1
rubygem20-psych-2.0.0-1.19.amzn1
ruby20-debuginfo-2.0.0.594-1.19.amzn1
ruby20-libs-2.0.0.594-1.19.amzn1
rubygem20-io-console-0.4.2-1.19.amzn1

i686
ruby20-libs-2.0.0.594-1.19.amzn1
ruby20-2.0.0.594-1.19.amzn1
ruby20-devel-2.0.0.594-1.19.amzn1
ruby20-debuginfo-2.0.0.594-1.19.amzn1
rubygem20-psych-2.0.0-1.19.amzn1
rubygem20-io-console-0.4.2-1.19.amzn1
rubygem20-bigdecimal-1.2.0-1.19.amzn1

noarch
rubygems20-2.0.14-1.19.amzn1
rubygems20-devel-2.0.14-1.19.amzn1
ruby20-doc-2.0.0.594-1.19.amzn1
ruby20-irb-2.0.0.594-1.19.amzn1

170415 - Amazon Linux AMI ALAS-2014-440 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4650

Description

The scan detected that the host is missing the following update:
ALAS-2014-440

Observation

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

https://alas.aws.amazon.com/ALAS-2014-440.html

Amazon Linux AMI
x86_64
python27-debuginfo-2.7.8-6.74.amzn1
python27-devel-2.7.8-6.74.amzn1
python27-test-2.7.8-6.74.amzn1
python27-2.7.8-6.74.amzn1
python27-libs-2.7.8-6.74.amzn1
python27-tools-2.7.8-6.74.amzn1

i686
python27-debuginfo-2.7.8-6.74.amzn1
python27-devel-2.7.8-6.74.amzn1
python27-2.7.8-6.74.amzn1
python27-tools-2.7.8-6.74.amzn1
python27-test-2.7.8-6.74.amzn1
python27-libs-2.7.8-6.74.amzn1

177987 - Gentoo Linux GLSA-201411-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0011

Description

The scan detected that the host is missing the following update:
GLSA-201411-03

Observation

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

http://security.gentoo.org/glsa/glsa-201411-03.xml

Affected packages:
net-misc/tigervnc < 1.3.1

181284 - FreeBSD Konversation Out-of-bounds Read On A Heap-allocated Array (0167f5ad-64ea-11e4-98c1-00269ee29e57)

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
Konversation -- out-of-bounds read on a heap-allocated array (0167f5ad-64ea-11e4-98c1-00269ee29e57)

Observation

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

http://www.vuxml.org/freebsd/0167f5ad-64ea-11e4-98c1-00269ee29e57.html

Affected packages:
konversation < 1.5.1

184606 - Ubuntu Linux 14.04, 14.10 USN-2404-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3657, CVE-2014-7823

Description

The scan detected that the host is missing the following update:
USN-2404-1

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-November/002722.html

Ubuntu 14.10

libvirt-bin_1.2.8-0ubuntu11.1
libvirt0_1.2.8-0ubuntu11.1

Ubuntu 14.04

libvirt0_1.2.2-0ubuntu13.1.7
libvirt-bin_1.2.2-0ubuntu13.1.7

184608 - Ubuntu Linux 12.04 USN-2401-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
USN-2401-1

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-November/002719.html

Ubuntu 12.04

konversation_1.4-1ubuntu2.1

184610 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2397-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080

Description

The scan detected that the host is missing the following update:
USN-2397-1

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-November/002715.html

Ubuntu 14.10

libruby2.1_2.1.2-2ubuntu1.1
ruby2.0_2.0.0.484+really457-3ubuntu1.1
libruby2.0_2.0.0.484+really457-3ubuntu1.1
ruby2.1_2.1.2-2ubuntu1.1

Ubuntu 14.04

libruby2.0_2.0.0.484-1ubuntu2.1
libruby1.9.1_1.9.3.484-2ubuntu1.1
ruby2.0_2.0.0.484-1ubuntu2.1
ruby1.9.1_1.9.3.484-2ubuntu1.1

Ubuntu 12.04

libruby1.8_1.8.7.352-2ubuntu1.5
ruby1.8_1.8.7.352-2ubuntu1.5
ruby1.9.1_1.9.3.0-1ubuntu2.9
libruby1.9.1_1.9.3.0-1ubuntu2.9

188435 - Fedora Linux 21 FEDORA-2014-13535 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13535

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143278.html

Fedora Core 21

file-5.19-7.fc21

188453 - Fedora Linux 21 FEDORA-2014-13831 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3623

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13831

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142593.html

Fedora Core 21

wss4j-1.6.17-1.fc21

188455 - Fedora Linux 19 FEDORA-2014-14043 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-2014-14043

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143323.html

Fedora Core 19

php-ZendFramework2-2.2.8-2.fc19

188468 - Fedora Linux 20 FEDORA-2014-13720 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3623

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13720

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142746.html

Fedora Core 20

wss4j-1.6.17-1.fc20

188473 - Fedora Linux 21 FEDORA-2014-12591 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-2014-12591

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142524.html

Fedora Core 21

bugzilla-4.4.6-1.fc21

188474 - Fedora Linux 21 FEDORA-2014-12341 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-2014-12341

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141794.html

Fedora Core 21

php-ZendFramework-1.12.9-1.fc21

188478 - Fedora Linux 21 FEDORA-2014-12915 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12915

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142592.html

Fedora Core 21

libxml2-2.9.1-6.fc21

188479 - Fedora Linux 21 FEDORA-2014-12483 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-2014-12483

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141821.html

Fedora Core 21

python-oauth2-1.5.211-8.fc21

188487 - Fedora Linux 21 FEDORA-2014-12947 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-2014-12947

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142006.html

Fedora Core 21

devscripts-2.14.10-1.fc21

188494 - Fedora Linux 21 FEDORA-2014-14096 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14096

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143151.html

Fedora Core 21

ruby-2.1.4-24.fc21

58992 - Debian Linux 7.0 DSA-3065-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2172

Description

The scan detected that the host is missing the following update:
DSA-3065-1

Observation

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

http://www.debian.org/security/2014/dsa-3065

Debian 7.0
all
libxml-security-java_1.4.5-1+deb7u1

142485 - SuSE Linux 13.2 openSUSE-SU-2014:1384-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

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

openSUSE-SU-2014:1384-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00030.html

SuSE Linux 13.2
i586
claws-mail-lang-3.11.0-2.4.1
claws-mail-debugsource-3.11.0-2.4.1
claws-mail-3.11.0-2.4.1
claws-mail-debuginfo-3.11.0-2.4.1
claws-mail-devel-3.11.0-2.4.1

142497 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1381-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7202, CVE-2014-7203

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1381-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00027.html

SuSE Linux 13.1
i586
zeromq-devel-4.0.5-4.4.3
zeromq-debugsource-4.0.5-4.4.3
libzmq4-4.0.5-4.4.3
libzmq4-debuginfo-4.0.5-4.4.3

SuSE Linux 12.3
i586
libzmq4-4.0.5-2.4.2
zeromq-devel-4.0.5-2.4.2
libzmq4-debuginfo-4.0.5-2.4.2
zeromq-debugsource-4.0.5-2.4.2

170419 - Amazon Linux AMI ALAS-2014-437 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7189

Description

The scan detected that the host is missing the following update:
ALAS-2014-437

Observation

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

https://alas.aws.amazon.com/ALAS-2014-437.html

Amazon Linux AMI
x86_64
golang-1.3.3-1.7.amzn1
golang-pkg-bin-linux-amd64-1.3.3-1.7.amzn1

i686
golang-pkg-bin-linux-386-1.3.3-1.7.amzn1
golang-1.3.3-1.7.amzn1

noarch
golang-src-1.3.3-1.7.amzn1
golang-pkg-netbsd-amd64-1.3.3-1.7.amzn1
golang-pkg-plan9-amd64-1.3.3-1.7.amzn1
golang-pkg-plan9-386-1.3.3-1.7.amzn1
golang-pkg-linux-amd64-1.3.3-1.7.amzn1
golang-pkg-linux-386-1.3.3-1.7.amzn1
golang-pkg-netbsd-386-1.3.3-1.7.amzn1
golang-pkg-darwin-amd64-1.3.3-1.7.amzn1
golang-pkg-openbsd-amd64-1.3.3-1.7.amzn1
golang-pkg-netbsd-arm-1.3.3-1.7.amzn1
golang-pkg-windows-386-1.3.3-1.7.amzn1
golang-pkg-freebsd-arm-1.3.3-1.7.amzn1
emacs-golang-1.3.3-1.7.amzn1
golang-pkg-freebsd-386-1.3.3-1.7.amzn1
golang-pkg-openbsd-386-1.3.3-1.7.amzn1
golang-vim-1.3.3-1.7.amzn1
golang-pkg-linux-arm-1.3.3-1.7.amzn1
golang-pkg-darwin-386-1.3.3-1.7.amzn1
golang-pkg-windows-amd64-1.3.3-1.7.amzn1
golang-pkg-freebsd-amd64-1.3.3-1.7.amzn1

184600 - Ubuntu Linux 14.04 USN-2406-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3621

Description

The scan detected that the host is missing the following update:
USN-2406-1

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-November/002724.html

Ubuntu 14.04

python-keystone_2014.1.3-0ubuntu2.1

184601 - Ubuntu Linux 14.04 USN-2405-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3641, CVE-2014-7230

Description

The scan detected that the host is missing the following update:
USN-2405-1

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-November/002723.html

Ubuntu 14.04

python-cinder_2014.1.3-0ubuntu1.1

184603 - Ubuntu Linux 12.04 USN-2400-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3575

Description

The scan detected that the host is missing the following update:
USN-2400-1

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-November/002718.html

Ubuntu 12.04

libreoffice-core_3.5.7-0ubuntu7

184609 - Ubuntu Linux 14.04 USN-2408-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6414

Description

The scan detected that the host is missing the following update:
USN-2408-1

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-November/002726.html

Ubuntu 14.04

python-neutron_2014.1.3-0ubuntu1.1

188427 - Fedora Linux 21 FEDORA-2014-12627 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-5356

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12627

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141840.html

Fedora Core 21

openstack-glance-2014.1.3-2.fc21

188438 - Fedora Linux 20 FEDORA-2014-13781 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13781

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142782.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142781.html

Fedora Core 20

subscription-manager-1.13.6-1.fc20
python-rhsm-1.13.6-1.fc20

188447 - Fedora Linux 21 FEDORA-2014-13647 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13647

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143170.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143169.html

Fedora Core 21

subscription-manager-1.13.6-1.fc21
python-rhsm-1.13.6-1.fc21

188450 - Fedora Linux 21 FEDORA-2014-13399 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13399

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142089.html

Fedora Core 21

asterisk-11.13.1-1.fc21

188451 - Fedora Linux 21 FEDORA-2014-12417 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3641

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12417

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142310.html

Fedora Core 21

openstack-cinder-2014.1.3-1.fc21

188456 - Fedora Linux 21 FEDORA-2014-13983 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4517

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13983

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143002.html

Fedora Core 21

xml-security-1.5.7-1.fc21

188457 - Fedora Linux 19 FEDORA-2014-13794 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13794

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142743.html

Fedora Core 19

python-rhsm-1.13.6-1.fc19

188462 - Fedora Linux 21 FEDORA-2014-14130 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7189

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14130

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143255.html

Fedora Core 21

golang-1.3.3-1.fc21

188467 - Fedora Linux 19 FEDORA-2014-13764 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2005-2090, CVE-2011-3389, CVE-2012-4929, CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13764

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142795.html

Fedora Core 19

Pound-2.6-8.fc19

188476 - Fedora Linux 21 FEDORA-2014-12951 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12951

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142330.html

Fedora Core 21

openssl-1.0.1j-1.fc21

188477 - Fedora Linux 21 FEDORA-2014-12955 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7970, CVE-2014-7975

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12955

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142017.html

Fedora Core 21

kernel-3.17.1-300.fc21

188491 - Fedora Linux 20 FEDORA-2014-13879 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4517

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13879

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142709.html

Fedora Core 20

xml-security-1.5.7-1.fc20

55236 - Top Weekly Malware Env - Trojan-rcaiarms (rcaiarms.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-rcaiarms (rcaiarms.exe)

Observation

This malware shows the following behavior:

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

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

58989 - Debian Linux 7.0 DSA-3067-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3689, CVE-2014-7815

Description

The scan detected that the host is missing the following update:
DSA-3067-1

Observation

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

http://www.debian.org/security/2014/dsa-3067

Debian 7.0
all
qemu-kvm_1.1.2+dfsg-6+deb7u5

58991 - Debian Linux 7.0 DSA-3069-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3707

Description

The scan detected that the host is missing the following update:
DSA-3069-1

Observation

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

http://www.debian.org/security/2014/dsa-3069

Debian 7.0
all
curl_7.26.0-1+wheezy11

58993 - Debian Linux 7.0 DSA-3066-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3689, CVE-2014-7815

Description

The scan detected that the host is missing the following update:
DSA-3066-1

Observation

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

http://www.debian.org/security/2014/dsa-3066

Debian 7.0

all
qemu_1.1.2+dfsg-6a+deb7u5

142495 - SuSE Linux 13.1, 13.2 openSUSE-SU-2014:1383-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8517

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1383-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00029.html

SuSE Linux 13.1
i586
tnftp-debuginfo-20100108-2.4.1
tnftp-debugsource-20100108-2.4.1
tnftp-20100108-2.4.1

SuSE Linux 13.2
i586
tnftp-debuginfo-20130505-4.4.1
tnftp-debugsource-20130505-4.4.1
tnftp-20130505-4.4.1

181285 - FreeBSD dbus Incomplete Fix For CVE-2014-3636 Part A (c1930f45-6982-11e4-80e1-bcaec565249c)

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

Risk Level: Low

CVE: CVE-2014-7824

Description

The scan detected that the host is missing the following update:
dbus -- incomplete fix for CVE-2014-3636 part A (c1930f45-6982-11e4-80e1-bcaec565249c)

Observation

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

http://www.vuxml.org/freebsd/c1930f45-6982-11e4-80e1-bcaec565249c.html

Affected packages:
dbus < 1.8.10

184599 - Ubuntu Linux 12.04 USN-2402-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8651

Description

The scan detected that the host is missing the following update:
USN-2402-1

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-November/002720.html

Ubuntu 12.04

kde-workspace-bin_4.8.5-0ubuntu0.4

184602 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2399-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3707

Description

The scan detected that the host is missing the following update:
USN-2399-1

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-November/002717.html

Ubuntu 14.10

libcurl3-gnutls_7.37.1-1ubuntu3.1
libcurl3-nss_7.37.1-1ubuntu3.1
libcurl3_7.37.1-1ubuntu3.1

Ubuntu 14.04

libcurl3_7.35.0-1ubuntu2.2
libcurl3-nss_7.35.0-1ubuntu2.2
libcurl3-gnutls_7.35.0-1ubuntu2.2

Ubuntu 12.04

libcurl3-gnutls_7.22.0-3ubuntu4.11
libcurl3_7.22.0-3ubuntu4.11
libcurl3-nss_7.22.0-3ubuntu4.11

Ubuntu 10.04

libcurl3-gnutls_7.19.7-1ubuntu1.10
libcurl3_7.19.7-1ubuntu1.10

184607 - Ubuntu Linux 14.10 USN-2403-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
USN-2403-1

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-November/002721.html

Ubuntu 14.10

gnutls-bin_3.2.16-1ubuntu2.1
libgnutlsxx28_3.2.16-1ubuntu2.1
libgnutls-openssl27_3.2.16-1ubuntu2.1
libgnutls-deb0-28_3.2.16-1ubuntu2.1

188423 - Fedora Linux 21 FEDORA-2014-14217 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-2014-14217

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143162.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143163.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143164.html

Fedora Core 21

claws-mail-3.11.1-2.fc21
claws-mail-plugins-3.11.1-1.fc21
libetpan-1.6-1.fc21

188424 - Fedora Linux 20 FEDORA-2014-14354 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3707

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14354

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143271.html

Fedora Core 20

curl-7.32.0-15.fc20

188430 - Fedora Linux 21 FEDORA-2014-12935 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-2014-12935

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142022.html

Fedora Core 21

java-1.8.0-openjdk-1.8.0.25-0.b18.fc21

188433 - Fedora Linux 21 FEDORA-2014-13632 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-2014-13632

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143240.html

Fedora Core 21

seamonkey-2.30-1.fc21

188436 - Fedora Linux 21 FEDORA-2014-13479 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-2014-13479

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142581.html

Fedora Core 21

phpMyAdmin-4.2.10.1-1.fc21

188437 - Fedora Linux 21 FEDORA-2014-14283 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8321, CVE-2014-8322, CVE-2014-8323, CVE-2014-8324

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14283

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143216.html

Fedora Core 21

aircrack-ng-1.2-0.5rc1.fc21

188440 - Fedora Linux 19 FEDORA-2014-13044 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-2014-13044

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142683.html

Fedora Core 19

thunderbird-31.2.0-1.fc19

188441 - Fedora Linux 21 FEDORA-2014-14084 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-2014-14084

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141796.html

Fedora Core 21

firefox-33.0-1.fc21

188442 - Fedora Linux 21 FEDORA-2014-12926 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-2014-12926

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142912.html

Fedora Core 21

zarafa-7.1.11-1.fc21

188443 - Fedora Linux 21 FEDORA-2014-14201 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-2014-14201

Observation

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

For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142914.html

Fedora Core 21

polarssl-1.3.9-1.fc21

188444 - Fedora Linux 21 FEDORA-2014-14208 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4616

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14208

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143191.html

Fedora Core 21

python3-3.4.1-16.fc21

188446 - Fedora Linux 21 FEDORA-2014-14347 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-6494

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14347

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142933.html

Fedora Core 21

fedup-0.9.0-2.fc21

188448 - Fedora Linux 20 FEDORA-2014-14241 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-2014-14241

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142686.html

Fedora Core 20

gnurobbo-0.66-4.20141028svn412.fc20

188449 - Fedora Linux 20 FEDORA-2014-14245 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4616

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14245

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142831.html

Fedora Core 20

python3-3.3.2-18.fc20

188454 - Fedora Linux 19 FEDORA-2014-13504 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-2014-13504

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141741.html

Fedora Core 19

phpMyAdmin-4.2.10.1-1.fc19

188458 - Fedora Linux 21 FEDORA-2014-14338 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3707

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14338

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143268.html

Fedora Core 21

curl-7.37.0-9.fc21

188459 - Fedora Linux 20 FEDORA-2014-14234 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-2014-14234

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143135.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143133.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143134.html

Fedora Core 20

claws-mail-plugins-3.11.1-1.fc20
claws-mail-3.11.1-2.fc20
libetpan-1.6-1.fc20

188460 - Fedora Linux 19 FEDORA-2014-13753 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-2014-13753

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142724.html

Fedora Core 19

seamonkey-2.30-1.fc19

188461 - Fedora Linux 19 FEDORA-2014-13017 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-2014-13017

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143267.html

Fedora Core 19

zarafa-7.1.11-1.fc19

188463 - Fedora Linux 20 FEDORA-2014-14033 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3689, CVE-2014-7815

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14033

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143312.html

Fedora Core 20

qemu-1.6.2-10.fc20

188465 - Fedora Linux 19 FEDORA-2014-13451 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-2014-13451

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142720.html

Fedora Core 19

webkitgtk3-2.0.4-4.fc19

188466 - Fedora Linux 21 FEDORA-2014-13993 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3689, CVE-2014-7815

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13993

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143107.html

Fedora Core 21

qemu-2.1.2-6.fc21

188469 - Fedora Linux 21 FEDORA-2014-13628 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-2014-13628

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143056.html

Fedora Core 21

Pound-2.7-0.4.d.fc21

188470 - Fedora Linux 21 FEDORA-2014-13461 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-2014-13461

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142139.html

Fedora Core 21

webkitgtk4-2.6.2-1.fc21

188471 - Fedora Linux 21 FEDORA-2014-13524 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-2014-13524

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142264.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142263.html

Fedora Core 21

webkitgtk-2.4.7-1.fc21
webkitgtk3-2.4.7-1.fc21

188472 - Fedora Linux 21 FEDORA-2014-12963 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-2014-12963

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142302.html

Fedora Core 21

deluge-1.3.10-1.fc21

188475 - Fedora Linux 19 FEDORA-2014-12994 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-2014-12994

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143374.html

Fedora Core 19

firefox-33.0-1.fc19

188480 - Fedora Linux 21 FEDORA-2014-12716 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-2014-12716

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142449.html

Fedora Core 21

perl-Mojolicious-5.49-1.fc21

188481 - Fedora Linux 20 FEDORA-2014-12989 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-2014-12989

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143105.html

Fedora Core 20

zarafa-7.1.11-1.fc20

188482 - Fedora Linux 20 FEDORA-2014-14227 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4650

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14227

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142835.html

Fedora Core 20

python-2.7.5-15.fc20

188484 - Fedora Linux 21 FEDORA-2014-12980 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-2014-12980

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142498.html

Fedora Core 21

rubygem-httpclient-2.4.0-2.fc21

188486 - Fedora Linux 21 FEDORA-2014-12940 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-2014-12940

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142587.html

Fedora Core 21

thunderbird-31.2.0-1.fc21

188488 - Fedora Linux 20 FEDORA-2014-14027 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-6494

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14027

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141698.html

Fedora Core 20

fedup-0.9.0-1.fc20

188490 - Fedora Linux 21 FEDORA-2014-12574 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-2014-12574

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/141823.html

Fedora Core 21

python-django-horizon-2014.1.3-1.fc21

188492 - Fedora Linux 19 FEDORA-2014-14252 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-6494

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14252

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/142698.html

Fedora Core 19

fedup-0.9.0-2.fc19

188493 - Fedora Linux 21 FEDORA-2014-14427 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-2014-14427

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143000.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143001.html

Fedora Core 21

freeipa-4.1.1-1.fc21
slapi-nis-0.54.1-1.fc21

184604 - Ubuntu Linux 14.04 USN-2407-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3608, CVE-2014-7230

Description

The scan detected that the host is missing the following update:
USN-2407-1

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-November/002725.html

Ubuntu 14.04

python-nova_2014.1.3-0ubuntu1.1

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

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

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 lnk 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 Ink 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

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

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

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

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

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

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

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

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

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

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

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

17357 - (MS14-066) Vulnerability in Schannel Could Allow Remote Code Execution (2992611)

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

Risk Level: High

CVE: CVE-2014-6321

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16347 - Microsoft Internet Explorer Flash ActionScript Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-0322

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

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

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

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

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

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

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

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

17362 - (MS14-064) Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)

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

Risk Level: High

CVE: CVE-2014-6332, CVE-2014-6352

Update Details

Recommendation is updated

17366 - (MS14-067) Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)

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

Risk Level: High

CVE: CVE-2014-4118

Update Details

Recommendation is updated

17372 - (MS14-065) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-4143

Update Details

Recommendation is updated

17373 - (MS14-065) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6337

Update Details

Recommendation is updated

17374 - (MS14-065) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6341

Update Details

Recommendation is updated

17375 - (MS14-065) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6342

Update Details

Recommendation is updated

17376 - (MS14-065) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6343

Update Details

Recommendation is updated

17377 - (MS14-065) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6344

Update Details

Recommendation is updated

17378 - (MS14-065) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6347

Update Details

Recommendation is updated

17379 - (MS14-065) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6348

Update Details

Recommendation is updated

17380 - (MS14-065) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6351

Update Details

Recommendation is updated

17381 - (MS14-065) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6353

Update Details

Recommendation is updated

17384 - (MS14-065) Cumulative Security Update for Internet Explorer (3003057)

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

Risk Level: High

CVE: CVE-2014-4143, CVE-2014-6323, CVE-2014-6337, CVE-2014-6339, CVE-2014-6340, CVE-2014-6341, CVE-2014-6342, CVE-2014-6343, CVE-2014-6344, CVE-2014-6345, CVE-2014-6346, CVE-2014-6347, CVE-2014-6348, CVE-2014-6349, CVE-2014-6350, CVE-2014-6351, CVE-2014-6353

Update Details

Recommendation is updated

17395 - (MS14-072) Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)

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

Risk Level: High

CVE: CVE-2014-4149

Update Details

Risk is updated

17399 - (MS14-073) Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)

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

Risk Level: High

CVE: CVE-2014-4116

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

30248 - Oracle Solaris 116973-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2005-3352, CVE-2006-3747, CVE-2006-5752, CVE-2007-3304, CVE-2007-5000, CVE-2007-6388, CVE-2009-0796, CVE-2011-0419, CVE-2011-1928, CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0053, CVE-2012-2687, CVE-2012-3499

Update Details

CVE 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17408 - (MS14-079) Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)

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

Risk Level: High

CVE: CVE-2014-6317

Update Details

Recommendation is updated

31007 - Oracle Solaris 116974-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2005-3352, CVE-2006-3747, CVE-2006-5752, CVE-2007-3304, CVE-2007-5000, CVE-2007-6388, CVE-2009-0796, CVE-2011-0419, CVE-2011-1928, CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0053, CVE-2012-2687, CVE-2012-3499

Update Details

CVE is updated

33116 - Oracle Solaris 150383-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Update Details

Risk is updated CVE 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FASLScript 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

FASLScript 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

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

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

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

17356 - (MS14-076) Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)

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

Risk Level: Medium

CVE: CVE-2014-4078

Update Details

Recommendation is updated

17359 - (MS14-076) Microsoft Internet Information Services IP And Domain Filtering List Security Bypass (2982998)

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

Risk Level: Medium

CVE: CVE-2014-4078

Update Details

Recommendation is updated

17360 - (MS14-066) Microsoft Windows Schannel Remote Code Execution (2992611)

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

Risk Level: Medium

CVE: CVE-2014-6321

Update Details

Recommendation is updated

17363 - (MS14-064) Microsoft Windows OLE Automation Array Remote Code Execution (3011443)

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

Risk Level: Medium

CVE: CVE-2014-6332

Update Details

Recommendation is updated

17364 - (MS14-064) Microsoft Windows OLE Remote Code Execution (3011443)

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

Risk Level: Medium

CVE: CVE-2014-6352

Update Details

Recommendation is updated

17365 - (MS14-065) Microsoft Internet Explorer ASLR Security Bypass (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6339

Update Details

Recommendation is updated

17367 - (MS14-065) Microsoft Internet Explorer Clipboard Information Disclosure (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6323

Update Details

Recommendation is updated

17368 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure I (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6340

Update Details

Recommendation is updated

17369 - (MS14-067) Microsoft Windows MSXML Core Services Remote Code Execution (2993958)

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

Risk Level: Medium

CVE: CVE-2014-4118

Update Details

Recommendation is updated

17370 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure II (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6345

Update Details

Recommendation is updated

17371 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure III (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6346

Update Details

Recommendation is updated

17382 - (MS14-065) Microsoft Internet Explorer Permission Validation I Privilege Escalation (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6349

Update Details

Recommendation is updated

17383 - (MS14-065) Microsoft Internet Explorer Permission Validation II Privilege Escalation (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6350

Update Details

Recommendation is updated

17386 - (MS14-069) Microsoft Word Invalid Pointer Remote Code Execution (3009710)

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

Risk Level: Medium

CVE: CVE-2014-6335

Update Details

Recommendation is updated

17387 - (MS14-069) Microsoft Word Bad Index Remote Code Execution (3009710)

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

Risk Level: Medium

CVE: CVE-2014-6334

Update Details

Recommendation is updated

17388 - (MS14-069) Microsoft Word Double Delete Remote Code Execution (3009710)

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

Risk Level: Medium

CVE: CVE-2014-6333

Update Details

Recommendation is updated

17390 - (MS14-071) Microsoft Windows Audio Services Privilege Escalation (3005607)

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

Risk Level: Medium

CVE: CVE-2014-6322

Update Details

Recommendation is updated

17391 - (MS14-070) Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)

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

Risk Level: Medium

CVE: CVE-2014-4076

Update Details

Recommendation is updated

17392 - (MS14-070) Microsoft Windows TCP/IP IOCTL Privilege Escalation (2989935)

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

Risk Level: Medium

CVE: CVE-2014-4076

Update Details

Recommendation is updated

17393 - (MS14-074) Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)

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

Risk Level: Medium

CVE: CVE-2014-6318

Update Details

Recommendation is updated

17394 - (MS14-074) Microsoft Windows Remote Desktop Protocol Audit Log Security Bypass (3003743)

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

Risk Level: Medium

CVE: CVE-2014-6318

Update Details

Recommendation is updated

17396 - (MS14-072) Microsoft .NET Framework Remoting TypeFilterLevel Privilege Escalation (3005210)

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

Risk Level: Medium

CVE: CVE-2014-4149

Update Details

Recommendation is updated

17397 - (MS14-078) Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)

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

Risk Level: Medium

CVE: CVE-2014-4077

Update Details

Recommendation is updated

17398 - (MS14-078) Microsoft Windows IME (Japanese) Privilege Escalation (2992719)

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

Risk Level: Medium

CVE: CVE-2014-4077

Update Details

Recommendation is updated

17400 - (MS14-073) Microsoft SharePoint Lists Privilege Escalation (3000431)

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

Risk Level: Medium

CVE: CVE-2014-4116

Update Details

Recommendation is updated

17407 - (MS14-077) Microsoft Active Directory Federation Services Information Disclosure (3003381)

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

Risk Level: Medium

CVE: CVE-2014-6331

Update Details

Recommendation is updated

17409 - (MS14-079) Microsoft Windows Kernel Denial of Service (3002885)

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

Risk Level: Medium

CVE: CVE-2014-6317

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

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

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

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

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

17389 - (MS14-071) Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)

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

Risk Level: Medium

CVE: CVE-2014-6322

Update Details

Recommendation is updated Risk 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

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

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

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

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

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

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

Update Details

FASLScript is updated

70083 - misc-network-id.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

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.