

## 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

#### 17514 - (HPSBUX03218) HP-UX Java Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-4288, CVE-2014-6456, CVE-2014-6457, CVE-2014-6458, CVE-2014-6466, CVE-2014-6476, CVE-2014-6492, CVE-2014-6493, CVE-2014-6502, CVE-2014-6503, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6515, CVE-2014-6517, CVE-2014-6519, CVE-2014-6527, CVE-2014-6531, CVE-2014-6558

#### Description

Multiple vulnerabilities are present in some versions of HP HP-UX.

#### Observation

HP HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP HP-UX. The flaws lie in the Java Runtime Environment (JRE) and the Java Developer Kit (JDK). Successful exploitation could allow an attacker to compromise a vulnerable system, disclose sensitive information, or cause a denial of service condition.

#### 142538 - SuSE SLES 11 SP3 java-1\_7\_0-ibm-9999 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3065, CVE-2014-3566, CVE-2014-4288, CVE-2014-6456, CVE-2014-6457, CVE-2014-6458, CVE-2014-6466, CVE-2014-6476, CVE-2014-6492, CVE-2014-6493, CVE-2014-6502, CVE-2014-6503, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6515, CVE-2014-6527, CVE-2014-6531, CVE-2014-6532, CVE-2014-6558

#### Description

The scan detected that the host is missing the following update:  
java-1\_7\_0-ibm-9999

#### Observation

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

[https://download.suse.com/Download?buildid=iigxv5kq\\_Do~](https://download.suse.com/Download?buildid=iigxv5kq_Do~)  
<https://download.suse.com/Download?buildid=9FYxmgibmQQ~>  
<https://download.suse.com/Download?buildid=CGxx4WGBAcg~>  
<https://download.suse.com/Download?buildid=WYGpsVC9r8l~>  
<https://download.suse.com/Download?buildid=0dCSpukg9Y0~>  
<https://download.suse.com/Download?buildid=N4YAkRPeY4g~>

SuSE SLES 11 SP3

x86\_64

java-1\_7\_0-ibm-alsa-1.7.0\_sr8.0-0.5.1

java-1\_7\_0-ibm-jdbc-1.7.0\_sr8.0-0.5.1  
java-1\_7\_0-ibm-1.7.0\_sr8.0-0.5.1  
java-1\_7\_0-ibm-plugin-1.7.0\_sr8.0-0.5.1

i586

java-1\_7\_0-ibm-alsa-1.7.0\_sr8.0-0.5.1  
java-1\_7\_0-ibm-jdbc-1.7.0\_sr8.0-0.5.1  
java-1\_7\_0-ibm-1.7.0\_sr8.0-0.5.1  
java-1\_7\_0-ibm-plugin-1.7.0\_sr8.0-0.5.1

## 142547 - SuSE SLES 11 SP3 java-1\_6\_0-ibm-9992 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3065, CVE-2014-3566, CVE-2014-4288, CVE-2014-6456, CVE-2014-6457, CVE-2014-6458, CVE-2014-6466, CVE-2014-6476, CVE-2014-6492, CVE-2014-6493, CVE-2014-6502, CVE-2014-6503, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6515, CVE-2014-6527, CVE-2014-6531, CVE-2014-6532, CVE-2014-6558

### Description

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

java-1\_6\_0-ibm-9992

### Observation

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

For more information see:

<https://download.suse.com/Download?buildid=Z49SpvM5VbQ~>  
[https://download.suse.com/Download?buildid=N2aolm7\\_FXw~](https://download.suse.com/Download?buildid=N2aolm7_FXw~)  
<https://download.suse.com/Download?buildid=oqf2gAJfCnU~>  
<https://download.suse.com/Download?buildid=Jsjl2h1pXPk~>  
<https://download.suse.com/Download?buildid=hCJydEAnY2M~>  
<https://download.suse.com/Download?buildid=Bv6gTHJc0NQ~>

SuSE SLES 11 SP3

x86\_64

java-1\_6\_0-ibm-fonts-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-jdbc-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-plugin-1.6.0\_sr16.2-0.3.1

i586

java-1\_6\_0-ibm-alsa-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-fonts-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-jdbc-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-1.6.0\_sr16.2-0.3.1  
java-1\_6\_0-ibm-plugin-1.6.0\_sr16.2-0.3.1

## 85834 - CentOS 5, 6, 7 CESA-2014-1919 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

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

CESA-2014-1919

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020796.html>  
<http://lists.centos.org/pipermail/centos-announce/2014-December/020798.html>  
<http://lists.centos.org/pipermail/centos-announce/2014-December/020801.html>

CentOS 7  
x86\_64  
firefox-31.3.0-3.el7.centos

i686  
firefox-31.3.0-3.el7.centos

CentOS 5  
x86\_64  
firefox-31.3.0-4.el5.centos

i386  
firefox-31.3.0-4.el5.centos

CentOS 6  
x86\_64  
firefox-31.3.0-3.el6.centos

i686  
firefox-31.3.0-3.el6.centos

## 91676 - Oracle Enterprise Linux ELSA-2014-3095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6407, CVE-2014-6408

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-3095

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004695.html>  
<http://oss.oracle.com/pipermail/el-errata/2014-December/004694.html>

OEL6  
x86\_64  
docker-pkg-devel-1.3.2-1.0.1.el6  
docker-1.3.2-1.0.1.el6  
docker-devel-1.3.2-1.0.1.el6

OEL7  
x86\_64  
docker-devel-1.3.2-1.0.1.el7  
docker-pkg-devel-1.3.2-1.0.1.el7  
docker-1.3.2-1.0.1.el7

## 91683 - Oracle Enterprise Linux ELSA-2014-1919 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1919

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004681.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004682.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004680.html>

#### OEL6

x86\_64

firefox-31.3.0-3.0.1.el6\_6

#### i386

firefox-31.3.0-3.0.1.el6\_6

#### OEL5

x86\_64

firefox-31.3.0-4.0.1.el5\_11

#### i386

firefox-31.3.0-4.0.1.el5\_11

#### OEL7

x86\_64

firefox-31.3.0-3.0.1.el7\_0

## 174604 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-706)

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-706)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=706>

#### SL7

x86\_64

firefox-31.3.0-3.el7\_0

firefox-debuginfo-31.3.0-3.el7\_0

SL6

x86\_64

firefox-debuginfo-31.3.0-3.el6\_6

firefox-31.3.0-3.el6\_6

i386

firefox-debuginfo-31.3.0-3.el6\_6

firefox-31.3.0-3.el6\_6

SL5

x86\_64

firefox-31.3.0-4.el5\_11

firefox-debuginfo-31.3.0-4.el5\_11

i386

firefox-31.3.0-4.el5\_11

firefox-debuginfo-31.3.0-4.el5\_11

## 188604 - Fedora Linux 21 FEDORA-2014-15347 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

### Description

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

FEDORA-2014-15347

### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145629.html>

Fedora Core 21

wget-1.16-3.fc21

## 17482 - (HPSBMU03074) HP Insight Control Server Migration Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2010-5298, CVE-2014-0076, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

### Description

Multiple vulnerabilities are present in some versions of HP Insight Control Server Migration.

### Observation

HP Insight Control Server Migration is a tool to migrate servers across different platforms.

Multiple vulnerabilities are present in some versions of HP Insight Control Server Migration. The flaws lie in the OpenSSL library. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service and execute arbitrary code.

## 178001 - Gentoo Linux GLSA-201412-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4292, CVE-2013-4296, CVE-2013-4297, CVE-2013-4399, CVE-2013-4400, CVE-2013-4401, CVE-2013-5651, CVE-2013-6436, CVE-2013-6456, CVE-2013-6457, CVE-2013-6458, CVE-2013-7336, CVE-2014-0028, CVE-2014-0179, CVE-2014-1447, CVE-2014-3633, CVE-2014-5177, CVE-2014-7823

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-04

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-04.xml>

Affected packages:

app-emulation/libvirt < 1.2.9-r2

## 85837 - CentOS 5, 6 CESA-2014-1924 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

The scan detected that the host is missing the following update:  
CESA-2014-1924

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020797.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020799.html>

CentOS 5

x86\_64

thunderbird-31.3.0-1.el5.centos

i386

thunderbird-31.3.0-1.el5.centos

CentOS 6

x86\_64

thunderbird-31.3.0-1.el6.centos

i686

thunderbird-31.3.0-1.el6.centos

## 85838 - CentOS 5, 6 CESA-2014-1974 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435

### Description

The scan detected that the host is missing the following update:  
CESA-2014-1974

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020819.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020818.html>

#### CentOS 5

x86\_64

rpm-apidocs-4.4.2.3-36.el5\_11

rpm-4.4.2.3-36.el5\_11

rpm-libs-4.4.2.3-36.el5\_11

rpm-devel-4.4.2.3-36.el5\_11

popt-1.10.2.3-36.el5\_11

rpm-python-4.4.2.3-36.el5\_11

rpm-build-4.4.2.3-36.el5\_11

i386

rpm-apidocs-4.4.2.3-36.el5\_11

rpm-4.4.2.3-36.el5\_11

rpm-libs-4.4.2.3-36.el5\_11

rpm-devel-4.4.2.3-36.el5\_11

popt-1.10.2.3-36.el5\_11

rpm-python-4.4.2.3-36.el5\_11

rpm-build-4.4.2.3-36.el5\_11

#### CentOS 6

x86\_64

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

i686

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

noarch

rpm-apidocs-4.8.0-38.el6\_6

rpm-cron-4.8.0-38.el6\_6

85839 - CentOS 5, 6, 7 CESA-2014-1948 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

## Description

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

CESA-2014-1948

## Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2014-December/020800.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020802.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020795.html>

### CentOS 7

x86\_64

nss-sysinit-3.16.2.3-2.el7\_0

nss-softokn-freebl-3.16.2.3-1.el7\_0

nss-softokn-freebl-devel-3.16.2.3-1.el7\_0

nss-pkcs11-devel-3.16.2.3-2.el7\_0

nss-softokn-devel-3.16.2.3-1.el7\_0

nss-3.16.2.3-2.el7\_0

nss-softokn-3.16.2.3-1.el7\_0

nss-util-3.16.2.3-1.el7\_0

nss-devel-3.16.2.3-2.el7\_0

nss-util-devel-3.16.2.3-1.el7\_0

nss-tools-3.16.2.3-2.el7\_0

i686

nss-softokn-freebl-3.16.2.3-1.el7\_0

nss-softokn-freebl-devel-3.16.2.3-1.el7\_0

nss-pkcs11-devel-3.16.2.3-2.el7\_0

nss-softokn-devel-3.16.2.3-1.el7\_0

nss-3.16.2.3-2.el7\_0

nss-softokn-3.16.2.3-1.el7\_0

nss-util-3.16.2.3-1.el7\_0

nss-devel-3.16.2.3-2.el7\_0

nss-util-devel-3.16.2.3-1.el7\_0

### CentOS 5

x86\_64

nss-pkcs11-devel-3.16.2.3-1.el5\_11

nss-tools-3.16.2.3-1.el5\_11

nss-3.16.2.3-1.el5\_11

nss-devel-3.16.2.3-1.el5\_11

i386

nss-pkcs11-devel-3.16.2.3-1.el5\_11

nss-tools-3.16.2.3-1.el5\_11

nss-3.16.2.3-1.el5\_11

nss-devel-3.16.2.3-1.el5\_11

### CentOS 6

x86\_64

nss-tools-3.16.2.3-3.el6\_6

nss-devel-3.16.2.3-3.el6\_6

nss-pkcs11-devel-3.16.2.3-3.el6\_6

nss-util-devel-3.16.2.3-2.el6\_6

nss-3.16.2.3-3.el6\_6

nss-util-3.16.2.3-2.el6\_6



nss-sysinit-3.16.2.3-3.el6\_6

i686

nss-tools-3.16.2.3-3.el6\_6

nss-devel-3.16.2.3-3.el6\_6

nss-pkcs11-devel-3.16.2.3-3.el6\_6

nss-util-devel-3.16.2.3-2.el6\_6

nss-3.16.2.3-3.el6\_6

nss-util-3.16.2.3-2.el6\_6

nss-sysinit-3.16.2.3-3.el6\_6

## 91678 - Oracle Enterprise Linux ELSA-2014-1974 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435

### Description

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

ELSA-2014-1974

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2014-December/004706.html>

OEL6

x86\_64

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-apidocs-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-cron-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

i386

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-apidocs-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-cron-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

## 91679 - Oracle Enterprise Linux ELSA-2014-1924 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

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

ELSA-2014-1924

## Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004679.html>

OEL6

x86\_64

thunderbird-31.3.0-1.0.1.el6\_6

i386

thunderbird-31.3.0-1.0.1.el6\_6

## 91680 - Oracle Enterprise Linux ELSA-2014-1948 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1568

## Description

The scan detected that the host is missing the following update:  
ELSA-2014-1948

## Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004676.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004677.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004678.html>

OEL6

x86\_64

nss-pkcs11-devel-3.16.2.3-3.0.1.el6\_6

nss-sysinit-3.16.2.3-3.0.1.el6\_6

nss-3.16.2.3-3.0.1.el6\_6

nss-util-3.16.2.3-2.el6\_6

nss-tools-3.16.2.3-3.0.1.el6\_6

nss-devel-3.16.2.3-3.0.1.el6\_6

nss-util-devel-3.16.2.3-2.el6\_6

i386

nss-pkcs11-devel-3.16.2.3-3.0.1.el6\_6

nss-sysinit-3.16.2.3-3.0.1.el6\_6

nss-3.16.2.3-3.0.1.el6\_6

nss-util-3.16.2.3-2.el6\_6

nss-tools-3.16.2.3-3.0.1.el6\_6

nss-devel-3.16.2.3-3.0.1.el6\_6

nss-util-devel-3.16.2.3-2.el6\_6

OEL5

x86\_64

nss-pkcs11-devel-3.16.2.3-1.el5\_11

nss-tools-3.16.2.3-1.el5\_11

nss-3.16.2.3-1.el5\_11

nss-devel-3.16.2.3-1.el5\_11

i386

nss-pkcs11-devel-3.16.2.3-1.el5\_11  
nss-tools-3.16.2.3-1.el5\_11  
nss-3.16.2.3-1.el5\_11  
nss-devel-3.16.2.3-1.el5\_11

## OEL7

x86\_64  
nss-softokn-freebl-3.16.2.3-1.el7\_0  
nss-softokn-freebl-devel-3.16.2.3-1.el7\_0  
nss-pkcs11-devel-3.16.2.3-2.0.1.el7\_0  
nss-softokn-devel-3.16.2.3-1.el7\_0  
nss-sysinit-3.16.2.3-2.0.1.el7\_0  
nss-softokn-3.16.2.3-1.el7\_0  
nss-tools-3.16.2.3-2.0.1.el7\_0  
nss-util-3.16.2.3-1.el7\_0  
nss-util-devel-3.16.2.3-1.el7\_0  
nss-3.16.2.3-2.0.1.el7\_0  
nss-devel-3.16.2.3-2.0.1.el7\_0

## 91681 - Oracle Enterprise Linux ELSA-2014-3096 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1739, CVE-2014-3181, CVE-2014-3184, CVE-2014-3185, CVE-2014-3535, CVE-2014-3601, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-3673, CVE-2014-3687, CVE-2014-4014, CVE-2014-4171, CVE-2014-4653, CVE-2014-4654, CVE-2014-4655

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-3096

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004686.html>  
<http://oss.oracle.com/pipermail/el-errata/2014-December/004685.html>

## OEL6

x86\_64  
kernel-uek-devel-3.8.13-55.el6uek  
kernel-uek-3.8.13-55.el6uek  
dtrace-modules-3.8.13-55.el6uek-0.4.3-4.el6  
kernel-uek-doc-3.8.13-55.el6uek  
kernel-uek-debug-devel-3.8.13-55.el6uek  
kernel-uek-debug-3.8.13-55.el6uek  
kernel-uek-firmware-3.8.13-55.el6uek

## OEL7

x86\_64  
kernel-uek-doc-3.8.13-55.el7uek  
kernel-uek-debug-3.8.13-55.el7uek  
kernel-uek-devel-3.8.13-55.el7uek  
kernel-uek-3.8.13-55.el7uek  
dtrace-modules-3.8.13-55.el7uek-0.4.3-4.el7  
kernel-uek-debug-devel-3.8.13-55.el7uek  
kernel-uek-firmware-3.8.13-55.el7uek

## 130010 - Debian Linux 7.0 DSA-3089-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9029

### Description

The scan detected that the host is missing the following update:  
DSA-3089-1

### Observation

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

<http://www.debian.org/security/2014/dsa-3089>

Debian 7.0

all

libjasper1\_1.900.1-13+deb7u1

libjasper-runtime\_1.900.1-13+deb7u1

libjasper-dev\_1.900.1-13+deb7u1

## 140633 - Red Hat Enterprise Linux RHSA-2014-1971 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2929, CVE-2014-1739, CVE-2014-3181, CVE-2014-3182, CVE-2014-3184, CVE-2014-3185, CVE-2014-3186, CVE-2014-3631, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4654, CVE-2014-4655, CVE-2014-4656, CVE-2014-5045, CVE-2014-6410

### Description

The scan detected that the host is missing the following update:  
RHSA-2014-1971

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1971.html>

RHEL7WS

x86\_64

kernel-debuginfo-3.10.0-123.13.1.el7

kernel-tools-debuginfo-3.10.0-123.13.1.el7

perf-3.10.0-123.13.1.el7

kernel-tools-3.10.0-123.13.1.el7

kernel-debuginfo-common-x86\_64-3.10.0-123.13.1.el7

kernel-debug-debuginfo-3.10.0-123.13.1.el7

kernel-3.10.0-123.13.1.el7

kernel-devel-3.10.0-123.13.1.el7

kernel-debug-devel-3.10.0-123.13.1.el7

kernel-debug-3.10.0-123.13.1.el7

python-perf-debuginfo-3.10.0-123.13.1.el7

kernel-headers-3.10.0-123.13.1.el7

kernel-tools-libs-3.10.0-123.13.1.el7

perf-debuginfo-3.10.0-123.13.1.el7

noarch  
kernel-abi-whitelists-3.10.0-123.13.1.el7

RHEL7D  
x86\_64  
kernel-debuginfo-3.10.0-123.13.1.el7  
kernel-tools-debuginfo-3.10.0-123.13.1.el7  
perf-3.10.0-123.13.1.el7  
kernel-tools-3.10.0-123.13.1.el7  
kernel-debuginfo-common-x86\_64-3.10.0-123.13.1.el7  
kernel-debug-debuginfo-3.10.0-123.13.1.el7  
kernel-3.10.0-123.13.1.el7  
kernel-devel-3.10.0-123.13.1.el7  
kernel-debug-devel-3.10.0-123.13.1.el7  
kernel-debug-3.10.0-123.13.1.el7  
python-perf-debuginfo-3.10.0-123.13.1.el7  
kernel-headers-3.10.0-123.13.1.el7  
kernel-tools-libs-3.10.0-123.13.1.el7  
perf-debuginfo-3.10.0-123.13.1.el7

noarch  
kernel-abi-whitelists-3.10.0-123.13.1.el7

RHEL7S  
x86\_64  
kernel-debuginfo-3.10.0-123.13.1.el7  
kernel-tools-debuginfo-3.10.0-123.13.1.el7  
perf-3.10.0-123.13.1.el7  
kernel-tools-3.10.0-123.13.1.el7  
kernel-debuginfo-common-x86\_64-3.10.0-123.13.1.el7  
kernel-debug-debuginfo-3.10.0-123.13.1.el7  
kernel-3.10.0-123.13.1.el7  
kernel-devel-3.10.0-123.13.1.el7  
kernel-debug-devel-3.10.0-123.13.1.el7  
kernel-debug-3.10.0-123.13.1.el7  
python-perf-debuginfo-3.10.0-123.13.1.el7  
kernel-headers-3.10.0-123.13.1.el7  
kernel-tools-libs-3.10.0-123.13.1.el7  
perf-debuginfo-3.10.0-123.13.1.el7

noarch  
kernel-abi-whitelists-3.10.0-123.13.1.el7

## 140634 - Red Hat Enterprise Linux RHSA-2014-1974 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435

### Description

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

RHSA-2014-1974

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2014-1974.html>

#### RHEL5D

x86\_64

rpm-python-4.4.2.3-36.el5\_11  
rpm-4.4.2.3-36.el5\_11  
rpm-libs-4.4.2.3-36.el5\_11  
popt-1.10.2.3-36.el5\_11  
rpm-debuginfo-4.4.2.3-36.el5\_11

i386

rpm-python-4.4.2.3-36.el5\_11  
rpm-4.4.2.3-36.el5\_11  
rpm-libs-4.4.2.3-36.el5\_11  
popt-1.10.2.3-36.el5\_11  
rpm-debuginfo-4.4.2.3-36.el5\_11

#### RHEL5S

x86\_64

rpm-devel-4.4.2.3-36.el5\_11  
rpm-4.4.2.3-36.el5\_11  
rpm-apidocs-4.4.2.3-36.el5\_11  
rpm-debuginfo-4.4.2.3-36.el5\_11  
rpm-build-4.4.2.3-36.el5\_11  
popt-1.10.2.3-36.el5\_11  
rpm-python-4.4.2.3-36.el5\_11  
rpm-libs-4.4.2.3-36.el5\_11

i386

rpm-devel-4.4.2.3-36.el5\_11  
rpm-4.4.2.3-36.el5\_11  
rpm-apidocs-4.4.2.3-36.el5\_11  
rpm-debuginfo-4.4.2.3-36.el5\_11  
rpm-build-4.4.2.3-36.el5\_11  
popt-1.10.2.3-36.el5\_11  
rpm-python-4.4.2.3-36.el5\_11  
rpm-libs-4.4.2.3-36.el5\_11

#### RHEL6D

x86\_64

rpm-python-4.8.0-38.el6\_6  
rpm-4.8.0-38.el6\_6  
rpm-debuginfo-4.8.0-38.el6\_6  
rpm-build-4.8.0-38.el6\_6  
rpm-libs-4.8.0-38.el6\_6

i386

rpm-python-4.8.0-38.el6\_6  
rpm-4.8.0-38.el6\_6  
rpm-debuginfo-4.8.0-38.el6\_6  
rpm-build-4.8.0-38.el6\_6  
rpm-libs-4.8.0-38.el6\_6

#### RHEL6S

x86\_64

rpm-python-4.8.0-38.el6\_6  
rpm-4.8.0-38.el6\_6  
rpm-debuginfo-4.8.0-38.el6\_6  
rpm-build-4.8.0-38.el6\_6  
rpm-libs-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

i386

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-debuginfo-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

RHEL6WS

x86\_64

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-debuginfo-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

i386

rpm-python-4.8.0-38.el6\_6

rpm-4.8.0-38.el6\_6

rpm-debuginfo-4.8.0-38.el6\_6

rpm-build-4.8.0-38.el6\_6

rpm-libs-4.8.0-38.el6\_6

rpm-devel-4.8.0-38.el6\_6

## 140636 - Red Hat Enterprise Linux RHSA-2014-1976 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

### Description

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

RHSA-2014-1976

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2014-1976.html>

RHEL7WS

x86\_64

rpm-build-libs-4.11.1-18.el7\_0

rpm-sign-4.11.1-18.el7\_0

rpm-4.11.1-18.el7\_0

rpm-devel-4.11.1-18.el7\_0

rpm-build-4.11.1-18.el7\_0

rpm-debuginfo-4.11.1-18.el7\_0

rpm-python-4.11.1-18.el7\_0

rpm-libs-4.11.1-18.el7\_0

RHEL7D

x86\_64

rpm-build-4.11.1-18.el7\_0

rpm-debuginfo-4.11.1-18.el7\_0

rpm-build-libs-4.11.1-18.el7\_0  
rpm-4.11.1-18.el7\_0  
rpm-libs-4.11.1-18.el7\_0  
rpm-python-4.11.1-18.el7\_0

RHEL7S

x86\_64  
rpm-build-libs-4.11.1-18.el7\_0  
rpm-sign-4.11.1-18.el7\_0  
rpm-4.11.1-18.el7\_0  
rpm-devel-4.11.1-18.el7\_0  
rpm-build-4.11.1-18.el7\_0  
rpm-debuginfo-4.11.1-18.el7\_0  
rpm-python-4.11.1-18.el7\_0  
rpm-libs-4.11.1-18.el7\_0

## 142542 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1588-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1588-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00034.html>

SuSE Linux 13.1

x86\_64  
libFLAC8-debuginfo-32bit-1.3.0-2.4.1  
libFLAC++6-debuginfo-32bit-1.3.0-2.4.1  
libFLAC8-32bit-1.3.0-2.4.1  
flac-devel-32bit-1.3.0-2.4.1  
libFLAC++6-32bit-1.3.0-2.4.1

i586

flac-debugsource-1.3.0-2.4.1  
libFLAC++6-1.3.0-2.4.1  
libFLAC++6-debuginfo-1.3.0-2.4.1  
libFLAC8-debuginfo-1.3.0-2.4.1  
flac-devel-1.3.0-2.4.1  
libFLAC8-1.3.0-2.4.1  
flac-1.3.0-2.4.1  
flac-debuginfo-1.3.0-2.4.1

SuSE Linux 12.3

x86\_64  
flac-devel-32bit-1.2.1\_git201212051942-3.4.1  
libFLAC++6-debuginfo-32bit-1.2.1\_git201212051942-3.4.1  
libFLAC++6-32bit-1.2.1\_git201212051942-3.4.1  
libFLAC8-debuginfo-32bit-1.2.1\_git201212051942-3.4.1  
libFLAC8-32bit-1.2.1\_git201212051942-3.4.1



i586  
flac-devel-1.2.1\_git201212051942-3.4.1  
libFLAC++6-1.2.1\_git201212051942-3.4.1  
flac-debuginfo-1.2.1\_git201212051942-3.4.1  
flac-debugsource-1.2.1\_git201212051942-3.4.1  
libFLAC8-debuginfo-1.2.1\_git201212051942-3.4.1  
flac-1.2.1\_git201212051942-3.4.1  
libFLAC8-1.2.1\_git201212051942-3.4.1  
libFLAC++6-debuginfo-1.2.1\_git201212051942-3.4.1

SuSE Linux 13.2

x86\_64  
libFLAC++6-debuginfo-32bit-1.3.0-4.4.1  
libFLAC8-debuginfo-32bit-1.3.0-4.4.1  
libFLAC8-32bit-1.3.0-4.4.1  
libFLAC++6-32bit-1.3.0-4.4.1  
flac-devel-32bit-1.3.0-4.4.1

i586  
flac-debuginfo-1.3.0-4.4.1  
flac-1.3.0-4.4.1  
flac-devel-1.3.0-4.4.1  
libFLAC8-1.3.0-4.4.1  
libFLAC++6-1.3.0-4.4.1  
libFLAC++6-debuginfo-1.3.0-4.4.1  
flac-debugsource-1.3.0-4.4.1  
libFLAC8-debuginfo-1.3.0-4.4.1

## 142545 - SuSE SLED 11 SP3 flash-player-10023 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8439

### Description

The scan detected that the host is missing the following update:  
flash-player-10023

### Observation

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

<https://download.suse.com/Download?buildid=9Np-R6EFSig~>  
<https://download.suse.com/Download?buildid=fhXS9GBIxfo~>

SuSE SLED 11 SP3

x86\_64  
flash-player-kde4-11.2.202.424-0.3.1  
flash-player-11.2.202.424-0.3.1  
flash-player-gnome-11.2.202.424-0.3.1

i586  
flash-player-kde4-11.2.202.424-0.3.1  
flash-player-11.2.202.424-0.3.1  
flash-player-gnome-11.2.202.424-0.3.1

## 142554 - SuSE SLED 11 SP3 libreoffice-2014-11-19-10001 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3693

### Description

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

libreoffice-2014-11-19-10001

### Observation

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

For more information see:

<https://download.suse.com/Download?buildid=8v6KyPssLul~>

<https://download.suse.com/Download?buildid=41BGP26IFt8~>

SuSE SLED 11 SP3

x86\_64

libreoffice-base-extensions-4.0.3.3.26-0.10.2

libreoffice-gnome-4.0.3.3.26-0.10.2

libreoffice-math-4.0.3.3.26-0.10.2

libreoffice-filters-optional-4.0.3.3.26-0.10.2

libreoffice-impress-4.0.3.3.26-0.10.2

libreoffice-kde-4.0.3.3.26-0.10.2

libreoffice-officebean-4.0.3.3.26-0.10.2

libreoffice-mono-4.0.3.3.26-0.10.2

libreoffice-impress-extensions-4.0.3.3.26-0.10.2

libreoffice-draw-4.0.3.3.26-0.10.2

libreoffice-4.0.3.3.26-0.10.2

libreoffice-kde4-4.0.3.3.26-0.10.2

libreoffice-calc-extensions-4.0.3.3.26-0.10.2

libreoffice-mailmerge-4.0.3.3.26-0.10.2

libreoffice-writer-extensions-4.0.3.3.26-0.10.2

libreoffice-pyuno-4.0.3.3.26-0.10.2

libreoffice-draw-extensions-4.0.3.3.26-0.10.2

libreoffice-calc-4.0.3.3.26-0.10.2

libreoffice-writer-4.0.3.3.26-0.10.2

libreoffice-base-4.0.3.3.26-0.10.2

libreoffice-base-drivers-postgresql-4.0.3.3.26-0.10.2

noarch

libreoffice-help-pl-4.0.3.3.26-0.10.2

libreoffice-l10n-hi-IN-4.0.3.3.26-0.10.1

libreoffice-help-ru-4.0.3.3.26-0.10.2

libreoffice-l10n-nn-4.0.3.3.26-0.10.1

libreoffice-l10n-pt-4.0.3.3.26-0.10.1

libreoffice-l10n-nl-4.0.3.3.26-0.10.1

libreoffice-help-it-4.0.3.3.26-0.10.2

libreoffice-l10n-ko-4.0.3.3.26-0.10.1

libreoffice-help-es-4.0.3.3.26-0.10.2

libreoffice-help-fr-4.0.3.3.26-0.10.2

libreoffice-help-zh-CN-4.0.3.3.26-0.10.2

libreoffice-help-nl-4.0.3.3.26-0.10.2

libreoffice-l10n-zh-CN-4.0.3.3.26-0.10.1

libreoffice-l10n-pl-4.0.3.3.26-0.10.1

libreoffice-l10n-xh-4.0.3.3.26-0.10.1

libreoffice-l10n-fi-4.0.3.3.26-0.10.1

libreoffice-help-cs-4.0.3.3.26-0.10.2

libreoffice-l10n-ja-4.0.3.3.26-0.10.1

libreoffice-l10n-ar-4.0.3.3.26-0.10.1

libreoffice-l10n-es-4.0.3.3.26-0.10.1  
libreoffice-l10n-zh-TW-4.0.3.3.26-0.10.1  
libreoffice-help-ja-4.0.3.3.26-0.10.2  
libreoffice-help-hu-4.0.3.3.26-0.10.2  
libreoffice-icon-themes-4.0.3.3.26-0.10.1  
libreoffice-help-en-US-4.0.3.3.26-0.10.2  
libreoffice-help-ko-4.0.3.3.26-0.10.2  
libreoffice-l10n-pt-BR-4.0.3.3.26-0.10.1  
libreoffice-l10n-it-4.0.3.3.26-0.10.1  
libreoffice-l10n-sv-4.0.3.3.26-0.10.1  
libreoffice-l10n-zu-4.0.3.3.26-0.10.1  
libreoffice-help-de-4.0.3.3.26-0.10.2  
libreoffice-l10n-ca-4.0.3.3.26-0.10.1  
libreoffice-l10n-da-4.0.3.3.26-0.10.1  
libreoffice-help-zh-TW-4.0.3.3.26-0.10.2  
libreoffice-l10n-ru-4.0.3.3.26-0.10.1  
libreoffice-l10n-af-4.0.3.3.26-0.10.1  
libreoffice-help-gu-IN-4.0.3.3.26-0.10.2  
libreoffice-l10n-gu-IN-4.0.3.3.26-0.10.1  
libreoffice-help-en-GB-4.0.3.3.26-0.10.2  
libreoffice-l10n-nb-4.0.3.3.26-0.10.1  
libreoffice-help-pt-4.0.3.3.26-0.10.2  
libreoffice-l10n-hu-4.0.3.3.26-0.10.1  
libreoffice-help-da-4.0.3.3.26-0.10.2  
libreoffice-l10n-sk-4.0.3.3.26-0.10.1  
libreoffice-l10n-fr-4.0.3.3.26-0.10.1  
libreoffice-l10n-de-4.0.3.3.26-0.10.1  
libreoffice-help-hi-IN-4.0.3.3.26-0.10.2  
libreoffice-help-pt-BR-4.0.3.3.26-0.10.2  
libreoffice-l10n-en-GB-4.0.3.3.26-0.10.1  
libreoffice-l10n-cs-4.0.3.3.26-0.10.1  
libreoffice-help-sv-4.0.3.3.26-0.10.2

i586

libreoffice-base-extensions-4.0.3.3.26-0.10.2  
libreoffice-gnome-4.0.3.3.26-0.10.2  
libreoffice-math-4.0.3.3.26-0.10.2  
libreoffice-filters-optional-4.0.3.3.26-0.10.2  
libreoffice-impress-4.0.3.3.26-0.10.2  
libreoffice-kde-4.0.3.3.26-0.10.2  
libreoffice-officebean-4.0.3.3.26-0.10.2  
libreoffice-mono-4.0.3.3.26-0.10.2  
libreoffice-impress-extensions-4.0.3.3.26-0.10.2  
libreoffice-draw-4.0.3.3.26-0.10.2  
libreoffice-4.0.3.3.26-0.10.2  
libreoffice-kde4-4.0.3.3.26-0.10.2  
libreoffice-calc-extensions-4.0.3.3.26-0.10.2  
libreoffice-mailmerge-4.0.3.3.26-0.10.2  
libreoffice-writer-extensions-4.0.3.3.26-0.10.2  
libreoffice-pyuno-4.0.3.3.26-0.10.2  
libreoffice-draw-extensions-4.0.3.3.26-0.10.2  
libreoffice-calc-4.0.3.3.26-0.10.2  
libreoffice-writer-4.0.3.3.26-0.10.2  
libreoffice-base-4.0.3.3.26-0.10.2  
libreoffice-base-drivers-postgresql-4.0.3.3.26-0.10.2

170432 - Amazon Linux AMI ALAS-2014-458 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

### Description

The scan detected that the host is missing the following update:  
ALAS-2014-458

### Observation

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

<https://alas.aws.amazon.com/ALAS-2014-458.html>

Amazon Linux AMI

x86\_64

rpm-debuginfo-4.11.2-2.58.amzn1

rpm-4.11.2-2.58.amzn1

rpm-python-4.11.2-2.58.amzn1

rpm-build-4.11.2-2.58.amzn1

rpm-sign-4.11.2-2.58.amzn1

rpm-libs-4.11.2-2.58.amzn1

rpm-devel-4.11.2-2.58.amzn1

rpm-build-libs-4.11.2-2.58.amzn1

i686

rpm-debuginfo-4.11.2-2.58.amzn1

rpm-python-4.11.2-2.58.amzn1

rpm-4.11.2-2.58.amzn1

rpm-build-4.11.2-2.58.amzn1

rpm-sign-4.11.2-2.58.amzn1

rpm-libs-4.11.2-2.58.amzn1

rpm-devel-4.11.2-2.58.amzn1

rpm-build-libs-4.11.2-2.58.amzn1

noarch

rpm-apidocs-4.11.2-2.58.amzn1

rpm-cron-4.11.2-2.58.amzn1

174601 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x i386/x86\_64 (1412-845)

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: thunderbird on SL6.x i386/x86\_64 (1412-845)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=845>

SL6

x86\_64

thunderbird-debuginfo-31.3.0-1.el6\_6

thunderbird-31.3.0-1.el6\_6

i386  
thunderbird-debuginfo-31.3.0-1.el6\_6  
thunderbird-31.3.0-1.el6\_6

### 181296 - FreeBSD freetype Out Of Bounds Stack-based Read/write (567beb1e-7e0a-11e4-b9cc-bcaec565249c)

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

Risk Level: High

CVE: CVE-2014-2240

#### Description

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

freetype -- Out of bounds stack-based read/write (567beb1e-7e0a-11e4-b9cc-bcaec565249c)

#### Observation

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

<http://www.vuxml.org/freebsd/567beb1e-7e0a-11e4-b9cc-bcaec565249c.html>

Affected packages:

freetype2 < 2.5.4

### 184633 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2434-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9029

#### Description

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

USN-2434-1

#### 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-December/002753.html>

Ubuntu 14.10

libjasper1\_1.900.1-debian1-2ubuntu0.1

Ubuntu 14.04

libjasper1\_1.900.1-14ubuntu3.1

Ubuntu 12.04

libjasper1\_1.900.1-13ubuntu0.1

### 184636 - Ubuntu Linux 10.04 USN-2434-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9029

#### Description

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

USN-2434-2

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002754.html>

Ubuntu 10.04

libgs8\_8.71.dfsg.1-0ubuntu5.6

184640 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2435-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

#### Description

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

USN-2435-1

#### 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-December/002755.html>

Ubuntu 14.10

graphviz\_2.38.0-5ubuntu0.1

Ubuntu 14.04

graphviz\_2.36.0-0ubuntu3.1

Ubuntu 12.04

graphviz\_2.26.3-10ubuntu1.2

Ubuntu 10.04

graphviz\_2.20.2-8ubuntu3.2

188566 - Fedora Linux 20 FEDORA-2014-14963 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-14963

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145262.html>

Fedora Core 20

avr-binutils-2.24-3.fc20

## 188567 - Fedora Linux 21 FEDORA-2014-14995 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-14995

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145328.html>

Fedora Core 21

avr-binutils-2.24-4.fc21

## 188569 - Fedora Linux 19 FEDORA-2014-5896 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2913

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-5896

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145738.html>

Fedora Core 19

nrpe-2.15-2.fc19

## 188570 - Fedora Linux 21 FEDORA-2014-14888 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-14888

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145352.html>

Fedora Core 21

arm-none-eabi-binutils-cs-2014.05.28-3.fc21

## 188571 - Fedora Linux 21 FEDORA-2014-15760 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15760

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145509.html>

Fedora Core 21

graphviz-2.38.0-11.fc21

## 188573 - Fedora Linux 21 FEDORA-2014-15338 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8990

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15338

### Observation

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



<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145357.html>

Fedora Core 21

lsyncd-2.1.5-6.fc21

### 188577 - Fedora Linux 20 FEDORA-2014-16258 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16258

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145728.html>

Fedora Core 20

flac-1.3.1-1.fc20

### 188583 - Fedora Linux 20 FEDORA-2014-14833 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-14833

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145256.html>

Fedora Core 20

arm-none-eabi-binutils-cs-2014.05.28-3.fc20

### 188603 - Fedora Linux 20 FEDORA-2014-15812 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

#### Description

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

FEDORA-2014-15812

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145217.html>

Fedora Core 20

graphviz-2.34.0-10.fc20

### 188606 - Fedora Linux 19 FEDORA-2014-15811 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15811

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145748.html>

Fedora Core 19

graphviz-2.30.1-13.fc19

### 188610 - Fedora Linux 19 FEDORA-2014-14838 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-14838

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145742.html>

Fedora Core 19

avr-binutils-2.24-3.fc19

### 188611 - Fedora Linux 19 FEDORA-2014-14874 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-14874

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145746.html>

Fedora Core 19

arm-none-eabi-binutils-cs-2014.05.28-3.fc19

### 85836 - CentOS 7 CESA-2014-1956 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

#### Description

The scan detected that the host is missing the following update:  
CESA-2014-1956

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020805.html>

CentOS 7

x86\_64

wpa\_supplicant-2.0-13.el7\_0

### 91677 - Oracle Enterprise Linux ELSA-2014-1956 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

#### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1956

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004683.html>

OEL7

x86\_64  
wpa\_supplicant-2.0-13.el7\_0

### 130009 - Debian Linux 7.0 DSA-3086-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8767, CVE-2014-8769, CVE-2014-9140

#### Description

The scan detected that the host is missing the following update:  
DSA-3086-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3086>

Debian 7.0  
all  
tcpdump\_4.3.0-1+deb7u1

### 130011 - Debian Linux 7.0 DSA-3085-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9031, CVE-2014-9033, CVE-2014-9034, CVE-2014-9035, CVE-2014-9036, CVE-2014-9037, CVE-2014-9038, CVE-2014-9039

#### Description

The scan detected that the host is missing the following update:  
DSA-3085-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3085>

Debian 7.0  
all  
wordpress\_3.6.1+dfsg-1~deb7u5

### 130012 - Debian Linux 7.0 DSA-3093-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7841, CVE-2014-8369, CVE-2014-8884, CVE-2014-9090

#### Description

The scan detected that the host is missing the following update:  
DSA-3093-1

## Observation

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

For more information see:

<http://www.debian.org/security/2014/dsa-3093>

Debian 7.0

all

nic-pcmcia-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
scsi-modules-3.2.0-4-s390x-di\_3.2.63-2+deb7u2  
crypto-dm-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
usb-modules-3.2.0-4-4kc-malta-di\_3.2.63-2+deb7u2  
nic-extra-modules-3.2.0-4-686-pae-di\_3.2.63-2+deb7u2  
crypto-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
btrfs-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
ext4-modules-3.2.0-4-itanium-di\_3.2.63-2+deb7u2  
isofs-modules-3.2.0-4-orion5x-di\_3.2.63-2+deb7u2  
usb-serial-modules-3.2.0-4-powerpc-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-powerpc-smp\_3.2.63-2+deb7u2  
btrfs-modules-3.2.0-4-r5k-ip32-di\_3.2.63-2+deb7u2  
scsi-core-modules-3.2.0-4-iop32x-di\_3.2.63-2+deb7u2  
kernel-image-3.2.0-4-r5k-cobalt-di\_3.2.63-2+deb7u2  
nic-usb-modules-3.2.0-4-loongson-2f-di\_3.2.63-2+deb7u2  
nfs-modules-3.2.0-4-r5k-cobalt-di\_3.2.63-2+deb7u2  
btrfs-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
kernel-image-3.2.0-4-versatile-di\_3.2.63-2+deb7u2  
crypto-modules-3.2.0-4-loongson-2f-di\_3.2.63-2+deb7u2  
uinput-modules-3.2.0-4-powerpc-di\_3.2.63-2+deb7u2  
usb-storage-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
parport-modules-3.2.0-4-itanium-di\_3.2.63-2+deb7u2  
ext2-modules-3.2.0-4-orion5x-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-rt-amd64-dbg\_3.2.63-2+deb7u2  
ext4-modules-3.2.0-4-s390x-di\_3.2.63-2+deb7u2  
isofs-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
nbd-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-powerpc-smp\_3.2.63-2+deb7u2  
nic-modules-3.2.0-4-itanium-di\_3.2.63-2+deb7u2  
multipath-modules-3.2.0-4-orion5x-di\_3.2.63-2+deb7u2  
fuse-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
isofs-modules-3.2.0-4-r4k-ip22-di\_3.2.63-2+deb7u2  
ext3-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
sata-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-s390x\_3.2.63-2+deb7u2  
serial-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
ppp-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-r5k-ip32\_3.2.63-2+deb7u2  
speakup-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
xfs-modules-3.2.0-4-itanium-di\_3.2.63-2+deb7u2  
scsi-core-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
sata-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-sb1-bcm91250a\_3.2.63-2+deb7u2  
qnx4-modules-3.2.0-4-686-pae-di\_3.2.63-2+deb7u2  
multipath-modules-3.2.0-4-powerpc-di\_3.2.63-2+deb7u2  
reiserfs-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
hfs-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
usb-storage-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-all-mipsel\_3.2.63-2+deb7u2  
input-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
crypto-dm-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
ext2-modules-3.2.0-4-itanium-di\_3.2.63-2+deb7u2

jfs-modules-3.2.0-4-loongson-2f-di\_3.2.63-2+deb7u2  
nbd-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
nic-shared-modules-3.2.0-4-r5k-cobalt-di\_3.2.63-2+deb7u2  
ext2-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
usb-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
uinput-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
xfs-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
usb-modules-3.2.0-4-iop32x-di\_3.2.63-2+deb7u2  
nic-modules-3.2.0-4-loongson-2f-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-powerpc64\_3.2.63-2+deb7u2  
nbd-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
core-modules-3.2.0-4-kirkwood-di\_3.2.63-2+deb7u2  
ext4-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
efi-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
minix-modules-3.2.0-4-orion5x-di\_3.2.63-2+deb7u2  
fuse-modules-3.2.0-4-686-pae-di\_3.2.63-2+deb7u2  
cdrom-core-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-all-sparc\_3.2.63-2+deb7u2  
input-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
udf-modules-3.2.0-4-loongson-2f-di\_3.2.63-2+deb7u2  
fat-modules-3.2.0-4-loongson-2f-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-r5k-ip32\_3.2.63-2+deb7u2  
squashfs-modules-3.2.0-4-kirkwood-di\_3.2.63-2+deb7u2  
sata-modules-3.2.0-4-powerpc-di\_3.2.63-2+deb7u2  
crypto-modules-3.2.0-4-versatile-di\_3.2.63-2+deb7u2  
fuse-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
ext2-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-iop32x\_3.2.63-2+deb7u2  
minix-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
udf-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
nic-wireless-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
crypto-dm-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
pcmcia-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
multipath-modules-3.2.0-4-r4k-ip22-di\_3.2.63-2+deb7u2  
nic-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
fuse-modules-3.2.0-4-4kc-malta-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-versatile\_3.2.63-2+deb7u2  
scsi-core-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
ata-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
usb-serial-modules-3.2.0-4-orion5x-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-sparc64\_3.2.63-2+deb7u2  
fat-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
ata-modules-3.2.0-4-powerpc-di\_3.2.63-2+deb7u2  
crc-modules-3.2.0-4-versatile-di\_3.2.63-2+deb7u2  
xfs-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
sata-modules-3.2.0-4-686-pae-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-all-i386\_3.2.63-2+deb7u2  
usb-storage-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
nic-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-r4k-ip22\_3.2.63-2+deb7u2  
nic-shared-modules-3.2.0-4-versatile-di\_3.2.63-2+deb7u2  
jfs-modules-3.2.0-4-mx5-di\_3.2.63-2+deb7u2  
ata-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
btrfs-modules-3.2.0-4-orion5x-di\_3.2.63-2+deb7u2  
ata-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
udf-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-amd64\_3.2.63-2+deb7u2  
reiserfs-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-all-s390\_3.2.63-2+deb7u2  
squashfs-modules-3.2.0-4-r5k-ip32-di\_3.2.63-2+deb7u2

jfs-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
fuse-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
md-modules-3.2.0-4-r5k-ip32-di\_3.2.63-2+deb7u2  
xfs-modules-3.2.0-4-sparc64-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-iop32x\_3.2.63-2+deb7u2  
scsi-extra-modules-3.2.0-4-powerpc-di\_3.2.63-2+deb7u2  
udf-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
linux-headers-3.2.0-4-r5k-cobalt\_3.2.63-2+deb7u2  
scsi-core-modules-3.2.0-4-kirkwood-di\_3.2.63-2+deb7u2  
nic-pcmcia-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-rt-686-pae\_3.2.63-2+deb7u2  
linux-image-3.2.0-4-kirkwood\_3.2.63-2+deb7u2  
squashfs-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
btrfs-modules-3.2.0-4-sb1-bcm91250a-di\_3.2.63-2+deb7u2  
leds-modules-3.2.0-4-kirkwood-di\_3.2.63-2+deb7u2  
kernel-image-3.2.0-4-r5k-ip32-di\_3.2.63-2+deb7u2  
multipath-modules-3.2.0-4-itanium-di\_3.2.63-2+deb7u2  
cdrom-core-modules-3.2.0-4-486-di\_3.2.63-2+deb7u2  
jfs-modules-3.2.0-4-4kc-malta-di\_3.2.63-2+deb7u2  
event-modules-3.2.0-4-amd64-di\_3.2.63-2+deb7u2  
ext2-modules-3.2.0-4-vexpress-di\_3.2.63-2+deb7u2  
floppy-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
virtio-modules-3.2.0-4-powerpc64-di\_3.2.63-2+deb7u2  
loop-modules-3.2.0-4-iop32x-di\_3.2.63-2+deb7u2  
hyperv-modules-3.2.0-4-686-pae-di\_3.2.63-2+deb7u2  
nic-shared-modules-3.2.0-4-r4k-ip22-di\_3.2.63-2+deb7u2  
crypto-dm-modules-3.2.0-4-686-pae-di\_3.2.63-2+deb7u2

### 130015 - Debian Linux 7.0 DSA-3091-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7273, CVE-2014-7274, CVE-2014-7275

#### Description

The scan detected that the host is missing the following update:  
DSA-3091-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3091>

Debian 7.0

all

getmail4\_4.46.0-1~deb7u1

### 140637 - Red Hat Enterprise Linux RHSA-2014-1956 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3686

#### Description

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

RHSA-2014-1956

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1956.html>

RHEL7WS

x86\_64  
wpa\_supplicant-debuginfo-2.0-13.el7\_0  
wpa\_supplicant-2.0-13.el7\_0

RHEL7D

x86\_64  
wpa\_supplicant-debuginfo-2.0-13.el7\_0  
wpa\_supplicant-2.0-13.el7\_0

RHEL7S

x86\_64  
wpa\_supplicant-debuginfo-2.0-13.el7\_0  
wpa\_supplicant-2.0-13.el7\_0

## 142540 - SuSE SLES 11 SP3, SLED 11 SP3 openvpn-10061 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

### Description

The scan detected that the host is missing the following update:  
openvpn-10061

### Observation

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

[https://download.suse.com/Download?buildid=5qgd\\_uTxtDs~](https://download.suse.com/Download?buildid=5qgd_uTxtDs~)  
<https://download.suse.com/Download?buildid=bFh0Cfem7pl~>  
[https://download.suse.com/Download?buildid=XO8s0\\_Y7\\_Xo~](https://download.suse.com/Download?buildid=XO8s0_Y7_Xo~)  
<https://download.suse.com/Download?buildid=9daobUUqeM0~>  
<https://download.suse.com/Download?buildid=eHjC3BL3QOM~>  
<https://download.suse.com/Download?buildid=74jdg0eDos~>  
[https://download.suse.com/Download?buildid=cfOe\\_MEgEt8~](https://download.suse.com/Download?buildid=cfOe_MEgEt8~)  
<https://download.suse.com/Download?buildid=m8UhseRGpCQ~>  
<https://download.suse.com/Download?buildid=nltLZFYeJKs~>

SuSE SLED 11 SP3

x86\_64  
openvpn-2.0.9-143.44.1

i586

openvpn-2.0.9-143.44.1

SuSE SLES 11 SP3

x86\_64  
openvpn-auth-pam-plugin-2.0.9-143.44.1



openvpn-2.0.9-143.44.1

i586

openvpn-auth-pam-plugin-2.0.9-143.44.1

openvpn-2.0.9-143.44.1

#### 142544 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1594-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

#### Description

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

openSUSE-SU-2014:1594-1

#### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00039.html>

SuSE Linux 13.1

i586

openvpn-auth-pam-plugin-2.3.2-3.4.1

openvpn-debuginfo-2.3.2-3.4.1

openvpn-down-root-plugin-2.3.2-3.4.1

openvpn-2.3.2-3.4.1

openvpn-down-root-plugin-debuginfo-2.3.2-3.4.1

openvpn-debugsource-2.3.2-3.4.1

openvpn-auth-pam-plugin-debuginfo-2.3.2-3.4.1

SuSE Linux 12.3

i586

openvpn-auth-pam-plugin-debuginfo-2.2.2-9.9.1

openvpn-2.2.2-9.9.1

openvpn-debugsource-2.2.2-9.9.1

openvpn-down-root-plugin-2.2.2-9.9.1

openvpn-down-root-plugin-debuginfo-2.2.2-9.9.1

openvpn-auth-pam-plugin-2.2.2-9.9.1

openvpn-debuginfo-2.2.2-9.9.1

SuSE Linux 13.2

i586

openvpn-auth-pam-plugin-debuginfo-2.3.4-2.4.1

openvpn-2.3.4-2.4.1

openvpn-auth-pam-plugin-2.3.4-2.4.1

openvpn-down-root-plugin-debuginfo-2.3.4-2.4.1

openvpn-debugsource-2.3.4-2.4.1

openvpn-down-root-plugin-2.3.4-2.4.1

openvpn-debuginfo-2.3.4-2.4.1

#### 142548 - SuSE SLES 11 SP3, SLED 11 SP3 python-2014-11-19-9996 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7185

## Description

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

python-2014-11-19-9996

## Observation

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

For more information see:

<https://download.suse.com/Download?buildid=EMuuDCKkozY~>

<https://download.suse.com/Download?buildid=xZ5tnvWzfsU~>

<https://download.suse.com/Download?buildid=NCqN8TIUkGQ~>

<https://download.suse.com/Download?buildid=7fdtxWtszdY~>

[https://download.suse.com/Download?buildid=gkeO04E\\_wXc~](https://download.suse.com/Download?buildid=gkeO04E_wXc~)

<https://download.suse.com/Download?buildid=68ioblyG5y8~>

<https://download.suse.com/Download?buildid=maWgLPpr6E0~>

<https://download.suse.com/Download?buildid=ZAimr6Vp8vQ~>

<https://download.suse.com/Download?buildid=nXPD-oFBk7w~>

### SuSE SLED 11 SP3

x86\_64

python-2.6.9-0.33.1

libpython2\_6-1\_0-2.6.9-0.33.1

python-base-2.6.9-0.33.1

python-xml-2.6.9-0.33.1

libpython2\_6-1\_0-32bit-2.6.9-0.33.1

python-tk-2.6.9-0.33.1

python-curses-2.6.9-0.33.1

python-devel-2.6.9-0.33.1

python-base-32bit-2.6.9-0.33.1

i586

python-2.6.9-0.33.1

python-tk-2.6.9-0.33.1

libpython2\_6-1\_0-2.6.9-0.33.1

python-devel-2.6.9-0.33.1

python-curses-2.6.9-0.33.1

python-base-2.6.9-0.33.1

python-xml-2.6.9-0.33.1

### SuSE SLES 11 SP3

x86\_64

python-2.6.9-0.33.1

libpython2\_6-1\_0-2.6.9-0.33.1

python-idle-2.6.9-0.33.1

python-base-2.6.9-0.33.1

python-demo-2.6.9-0.33.1

python-xml-2.6.9-0.33.1

libpython2\_6-1\_0-32bit-2.6.9-0.33.1

python-tk-2.6.9-0.33.1

python-gdbm-2.6.9-0.33.1

python-32bit-2.6.9-0.33.1

python-curses-2.6.9-0.33.1

python-base-32bit-2.6.9-0.33.1

noarch

python-doc-2.6-8.33.1

python-doc-pdf-2.6-8.33.1

i586  
python-2.6.9-0.33.1  
libpython2\_6-1\_0-2.6.9-0.33.1  
python-idle-2.6.9-0.33.1  
python-base-2.6.9-0.33.1  
python-demo-2.6.9-0.33.1  
python-xml-2.6.9-0.33.1  
python-tk-2.6.9-0.33.1  
python-gdbm-2.6.9-0.33.1  
python-curses-2.6.9-0.33.1

## 142553 - SuSE SLED 11 SP3 compat-openssl097g-10033 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0166, CVE-2013-0169, CVE-2014-0224, CVE-2014-3470, CVE-2014-3508, CVE-2014-3566, CVE-2014-3568

### Description

The scan detected that the host is missing the following update:  
compat-openssl097g-10033

### Observation

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

<https://download.suse.com/Download?buildid=IQZHNCnTzjw~>  
<https://download.suse.com/Download?buildid=PuqtzJm-wyM~>

SuSE SLED 11 SP3  
x86\_64  
compat-openssl097g-0.9.7g-146.22.25.1  
compat-openssl097g-32bit-0.9.7g-146.22.25.1

i586  
compat-openssl097g-0.9.7g-146.22.25.1

## 170434 - Amazon Linux AMI ALAS-2014-456 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3248

### Description

The scan detected that the host is missing the following update:  
ALAS-2014-456

### Observation

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

<https://alas.aws.amazon.com/ALAS-2014-456.html>

Amazon Linux AMI  
noarch  
facter-1.6.18-7.25.amzn1

## 174600 - Scientific Linux Security ERRATA Moderate: wpa\_supplicant on SL7.x x86\_64 (1412-975)

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

Risk Level: Medium

CVE: CVE-2014-3686

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Moderate: wpa\_supplicant on SL7.x x86\_64 (1412-975)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=975>

SL7

x86\_64

wpa\_supplicant-debuginfo-2.0-13.el7\_0

wpa\_supplicant-2.0-13.el7\_0

## 177998 - Gentoo Linux GLSA-201412-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3471, CVE-2014-3615, CVE-2014-3640, CVE-2014-5263, CVE-2014-5388, CVE-2014-7815

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-01

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-01.xml>

Affected packages:

app-emulation/qemu < 2.1.2-r1

## 184639 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2433-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8767, CVE-2014-8768, CVE-2014-8769, CVE-2014-9140

### Description

The scan detected that the host is missing the following update:  
USN-2433-1

### 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-December/002751.html>

Ubuntu 14.10

tcpdump\_4.6.2-1ubuntu1.1

Ubuntu 14.04

tcpdump\_4.5.1-2ubuntu1.1

Ubuntu 12.04

tcpdump\_4.2.1-1ubuntu2.1

Ubuntu 10.04

tcpdump\_4.0.0-6ubuntu3.1

### 188568 - Fedora Linux 21 FEDORA-2014-15588 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8958, CVE-2014-8959, CVE-2014-8960, CVE-2014-8961

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15588

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145389.html>

Fedora Core 21

phpMyAdmin-4.2.12-1.fc21

### 188574 - Fedora Linux 21 FEDORA-2014-15560 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9031, CVE-2014-9032, CVE-2014-9033, CVE-2014-9034, CVE-2014-9035, CVE-2014-9036, CVE-2014-9037, CVE-2014-9038, CVE-2014-9039

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15560

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145372.html>

Fedora Core 21

wordpress-4.0.1-1.fc21

### 188578 - Fedora Linux 21 FEDORA-2014-15630 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-6662, CVE-2014-9015

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15630

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145571.html>

Fedora Core 21

drupal6-6.34-1.fc21

### 188593 - Fedora Linux 21 FEDORA-2014-15609 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8767, CVE-2014-8768, CVE-2014-8769

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15609

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145449.html>

Fedora Core 21

tcpdump-4.6.2-2.fc21

### 188595 - Fedora Linux 19 FEDORA-2014-15549 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8767, CVE-2014-8769

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15549

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145201.html>

Fedora Core 19

tcpdump-4.4.0-4.fc19

### 17040 - IBM Domino Apache Commons FileUpload Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-0050

#### Description

A denial of service vulnerability is present in some versions of IBM Domino Server.

#### Observation

IBM Domino Server is a business collaboration software.

A denial of service vulnerability is present in some versions of IBM Domino Server. The flaw lies within the Apache Commons FileUpload component of the Domino web server. Successful exploitation could allow an attacker to cause a denial of service condition by sending specially crafted requests that makes the server to enter into an infinite loop.

### 17454 - Splunk Enterprise OpenSSL Denial of Service Vulnerability Prior To 6.1.5

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

Risk Level: Medium

CVE: CVE-2014-3567

#### Description

A denial of service vulnerability is present in some versions of Splunk Enterprise.

#### Observation

Splunk Enterprise is a cloud application for collecting, indexing and harnessing all the fast moving machine data.

A denial of service vulnerability is present in some versions of Splunk Enterprise. The flaw lies in the OpenSSL library. Successful exploitation could allow an attacker to cause a denial of service.

### 17465 - IDA Pro Memory Corruption Vulnerability (2014-11-25)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Description

A remote code execution vulnerability is present in some versions of Hex-Rays IDA Pro Disassembler.

#### Observation

Hex-Rays IDA Pro Disassembler is a popular disassembler and debugger.

A remote code execution vulnerability is present in some versions of Hex-Rays IDA Pro Disassembler. The flaw lies in memory management of EPOC, ELF and PE files by Hex-Rays IDA Pro Disassembler. As a result, an attacker may execute arbitrary code. An attacker must beguile the victim into opening a malicious file.

## 17474 - (SOL15862) F5 BIG-IP Multiple cURL and libcurl Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-0015, CVE-2014-0138, CVE-2014-0139

### Description

Multiple 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 vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in cURL and libcurl. Successful exploitation could allow unauthorized disclosure of information and unauthorized modification.

## 140635 - Red Hat Enterprise Linux RHSA-2014-1972 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5704, CVE-2014-3581

### Description

The scan detected that the host is missing the following update:  
RHSA-2014-1972

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2014-1972.html>

RHEL7WS

x86\_64

httpd24-httpd-tools-2.4.6-25.el7

httpd24-httpd-2.4.6-25.el7

httpd24-mod\_session-2.4.6-25.el7

httpd24-httpd-devel-2.4.6-25.el7

httpd24-mod\_proxy\_html-2.4.6-25.el7

httpd24-mod\_ssl-2.4.6-25.el7

httpd24-mod\_ldap-2.4.6-25.el7

httpd24-httpd-debuginfo-2.4.6-25.el7

noarch

httpd24-httpd-manual-2.4.6-25.el7

RHEL7S

x86\_64

httpd24-httpd-tools-2.4.6-25.el7

httpd24-httpd-2.4.6-25.el7

httpd24-mod\_session-2.4.6-25.el7

httpd24-httpd-devel-2.4.6-25.el7



httpd24-mod\_proxy\_html-2.4.6-25.el7  
httpd24-mod\_ssl-2.4.6-25.el7  
httpd24-mod\_ldap-2.4.6-25.el7  
httpd24-httpd-debuginfo-2.4.6-25.el7

noarch  
httpd24-httpd-manual-2.4.6-25.el7

RHEL6S  
x86\_64  
httpd24-mod\_proxy\_html-2.4.6-22.el6  
httpd24-mod\_session-2.4.6-22.el6  
httpd24-httpd-devel-2.4.6-22.el6  
httpd24-httpd-debuginfo-2.4.6-22.el6  
httpd24-mod\_ldap-2.4.6-22.el6  
httpd24-httpd-2.4.6-22.el6  
httpd24-mod\_ssl-2.4.6-22.el6  
httpd24-httpd-tools-2.4.6-22.el6

noarch  
httpd24-httpd-manual-2.4.6-22.el6

RHEL6WS  
x86\_64  
httpd24-mod\_proxy\_html-2.4.6-22.el6  
httpd24-mod\_session-2.4.6-22.el6  
httpd24-httpd-devel-2.4.6-22.el6  
httpd24-httpd-debuginfo-2.4.6-22.el6  
httpd24-mod\_ldap-2.4.6-22.el6  
httpd24-httpd-2.4.6-22.el6  
httpd24-mod\_ssl-2.4.6-22.el6  
httpd24-httpd-tools-2.4.6-22.el6

noarch  
httpd24-httpd-manual-2.4.6-22.el6

## 142537 - SuSE SLES 11 SP3, SLED 11 SP3 clamav-10016 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6497, CVE-2014-9050

### Description

The scan detected that the host is missing the following update:  
clamav-10016

### Observation

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

<https://download.suse.com/Download?buildid=4llxuwYsD9Q~>  
<https://download.suse.com/Download?buildid=icMoY1-EHFE~>  
<https://download.suse.com/Download?buildid=nIORHIV6Kpc~>  
<https://download.suse.com/Download?buildid=cSHidrfdOio~>  
<https://download.suse.com/Download?buildid=VaVGsmtDcSE~>  
<https://download.suse.com/Download?buildid=rZL25XAw5nM~>  
<https://download.suse.com/Download?buildid=EfG-GSj226I~>  
<https://download.suse.com/Download?buildid=90GEYN1K6HU~>

[https://download.suse.com/Download?buildid=\\_Zs3ISHLIFE~](https://download.suse.com/Download?buildid=_Zs3ISHLIFE~)

SuSE SLED 11 SP3  
x86\_64  
clamav-0.98.5-0.5.1

i586  
clamav-0.98.5-0.5.1

SuSE SLES 11 SP3  
x86\_64  
clamav-0.98.5-0.5.1

i586  
clamav-0.98.5-0.5.1

#### 142541 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1589-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8080, CVE-2014-8090

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1589-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00035.html>

SuSE Linux 13.1  
i586

ruby19-tk-1.9.3.p448-2.8.1  
ruby19-1.9.3.p448-2.8.1  
ruby19-debuginfo-1.9.3.p448-2.8.1  
ruby19-doc-ri-1.9.3.p448-2.8.1  
ruby19-devel-extra-1.9.3.p448-2.8.1  
ruby19-devel-1.9.3.p448-2.8.1  
ruby19-tk-debuginfo-1.9.3.p448-2.8.1  
ruby19-debugsource-1.9.3.p448-2.8.1

SuSE Linux 12.3  
i586

ruby19-debuginfo-1.9.3.p392-1.21.1  
ruby19-devel-extra-1.9.3.p392-1.21.1  
ruby19-1.9.3.p392-1.21.1  
ruby19-doc-ri-1.9.3.p392-1.21.1  
ruby19-debugsource-1.9.3.p392-1.21.1  
ruby19-devel-1.9.3.p392-1.21.1  
ruby19-tk-debuginfo-1.9.3.p392-1.21.1  
ruby19-tk-1.9.3.p392-1.21.1

#### 142543 - SuSE SLES 10 SP4 clamav-9001 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6497, CVE-2014-9050

#### Description

The scan detected that the host is missing the following update:  
clamav-9001

#### Observation

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

<https://download.suse.com/Download?buildid=7NND0YpiZMM~>  
<https://download.suse.com/Download?buildid=o1h6TebFM8M~>  
<https://download.suse.com/Download?buildid=bfFB-1QsznU~>

SuSE SLES 10 SP4  
x86\_64  
clamav-0.98.5-0.7.1

i586  
clamav-0.98.5-0.7.1

### 142546 - SuSE Linux 13.2 openSUSE-SU-2014:1596-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6407, CVE-2014-6408

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1596-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00040.html>

SuSE Linux 13.2  
x86\_64  
docker-debuginfo-1.3.2-9.1  
docker-1.3.2-9.1  
docker-debugsource-1.3.2-9.1  
docker-bash-completion-1.3.2-9.1  
docker-zsh-completion-1.3.2-9.1

### 142549 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1591-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9018, CVE-2014-9091

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1591-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00037.html>

SuSE Linux 13.1

i586

icecast-debuginfo-2.3.3-2.12.1

icecast-debugsource-2.3.3-2.12.1

icecast-2.3.3-2.12.1

icecast-doc-2.3.3-2.12.1

SuSE Linux 12.3

i586

icecast-debuginfo-2.3.2-72.4.1

icecast-debugsource-2.3.2-72.4.1

icecast-2.3.2-72.4.1

### 142550 - SuSE Linux 13.2 openSUSE-SU-2014:1593-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9018

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1593-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00038.html>

SuSE Linux 13.2

i586

icecast-debugsource-2.4.0-2.8.1

icecast-debuginfo-2.4.0-2.8.1

icecast-doc-2.4.0-2.8.1

icecast-2.4.0-2.8.1

### 142552 - SuSE SLES 11 SP2 clamav-10015 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2020, CVE-2013-2021, CVE-2013-6497, CVE-2014-9050

### Description

The scan detected that the host is missing the following update:  
clamav-10015

### Observation

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

For more information see:

<https://download.suse.com/Download?buildid=D17s2KkMWeU~>

<https://download.suse.com/Download?buildid=s7rBHFvZg0g~>

[https://download.suse.com/Download?buildid=qeaatc0\\_7XQ~](https://download.suse.com/Download?buildid=qeaatc0_7XQ~)

SuSE SLES 11 SP2

x86\_64

clamav-0.98.5-0.5.1

i586

clamav-0.98.5-0.5.1

## 142556 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1560-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6497, CVE-2014-9050

### Description

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

openSUSE-SU-2014:1560-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00016.html>

SuSE Linux 13.1

i586

clamav-debugsource-0.98.5-22.3

clamav-0.98.5-22.3

clamav-debuginfo-0.98.5-22.3

SuSE Linux 12.3

i586

clamav-0.98.5-5.30.3

clamav-debuginfo-0.98.5-5.30.3

clamav-debugsource-0.98.5-5.30.3

SuSE Linux 13.2

i586

clamav-0.98.5-2.5.2

clamav-debuginfo-0.98.5-2.5.2

clamav-debugsource-0.98.5-2.5.2

## 170435 - Amazon Linux AMI ALAS-2014-455 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7841, CVE-2014-7970

### Description

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

ALAS-2014-455

### Observation

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

<https://alas.aws.amazon.com/ALAS-2014-455.html>

#### Amazon Linux AMI

x86\_64  
kernel-devel-3.14.25-23.45.amzn1  
kernel-tools-debuginfo-3.14.25-23.45.amzn1  
kernel-debuginfo-3.14.25-23.45.amzn1  
perf-3.14.25-23.45.amzn1  
kernel-debuginfo-common-x86\_64-3.14.25-23.45.amzn1  
perf-debuginfo-3.14.25-23.45.amzn1  
kernel-headers-3.14.25-23.45.amzn1  
kernel-tools-3.14.25-23.45.amzn1  
kernel-3.14.25-23.45.amzn1  
kernel-tools-devel-3.14.25-23.45.amzn1

#### i686

kernel-devel-3.14.25-23.45.amzn1  
kernel-tools-debuginfo-3.14.25-23.45.amzn1  
kernel-debuginfo-common-i686-3.14.25-23.45.amzn1  
kernel-debuginfo-3.14.25-23.45.amzn1  
perf-3.14.25-23.45.amzn1  
perf-debuginfo-3.14.25-23.45.amzn1  
kernel-headers-3.14.25-23.45.amzn1  
kernel-tools-3.14.25-23.45.amzn1  
kernel-3.14.25-23.45.amzn1  
kernel-tools-devel-3.14.25-23.45.amzn1

#### noarch

kernel-doc-3.14.25-23.45.amzn1

### 177997 - Gentoo Linux GLSA-201412-05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9050

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-05

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-05.xml>

Affected packages:

app-antivirus/clamav < 0.98.5

### 178000 - Gentoo Linux GLSA-201412-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3430

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-03

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-03.xml>

Affected packages:

net-mail/dovecot < 2.2.13

181298 - FreeBSD phpMyAdmin XSS And DoS Vulnerabilities (c9c46fbf-7b83-11e4-a96e-6805ca0b3d42)

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

Risk Level: Medium

CVE: CVE-2014-9218, CVE-2014-9219

#### Description

The scan detected that the host is missing the following update:  
phpMyAdmin -- XSS and DoS vulnerabilities (c9c46fbf-7b83-11e4-a96e-6805ca0b3d42)

#### Observation

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

<http://www.vuxml.org/freebsd/c9c46fbf-7b83-11e4-a96e-6805ca0b3d42.html>

Affected packages:

4.2.0 <= phpMyAdmin < 4.2.13.1

184632 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2432-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-6656, CVE-2014-6040, CVE-2014-7817

#### Description

The scan detected that the host is missing the following update:  
USN-2432-1

#### 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-December/002750.html>

Ubuntu 14.10

libc6\_2.19-10ubuntu2.1

Ubuntu 14.04

libc6\_2.19-0ubuntu6.4

Ubuntu 12.04

libc6\_2.15-0ubuntu10.9

Ubuntu 10.04

libc6\_2.11.1-0ubuntu7.19

#### 188581 - Fedora Linux 21 FEDORA-2014-15863 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15863

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145508.html>

Fedora Core 21

libksba-1.3.2-1.fc21

#### 188585 - Fedora Linux 21 FEDORA-2014-15434 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6497, CVE-2014-9050

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15434

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145507.html>

Fedora Core 21

clamav-0.98.5-1.fc21

#### 188588 - Fedora Linux 21 FEDORA-2014-15583 Update Is Not Installed



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

Risk Level: Medium

CVE: CVE-2014-9016

#### Description

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

FEDORA-2014-15583

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145329.html>

Fedora Core 21

drupal7-7.34-1.fc21

### 188598 - Fedora Linux 20 FEDORA-2014-15847 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

#### Description

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

FEDORA-2014-15847

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145241.html>

Fedora Core 20

libsba-1.3.2-1.fc20

### 188599 - Fedora Linux 21 FEDORA-2014-15320 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714

#### Description

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

FEDORA-2014-15320

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145658.html>

Fedora Core 21

wireshark-1.12.2-1.fc21

### 188600 - Fedora Linux 19 FEDORA-2014-15838 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15838

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145745.html>

Fedora Core 19

libksba-1.3.2-1.fc19

### 188605 - Fedora Linux 20 FEDORA-2014-15244 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15244

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145174.html>

Fedora Core 20

wireshark-1.10.11-1.fc20

### 17523 - (SOL15882) F5 BIG-IP TLS1.x Padding Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-8730

#### Description

An information disclosure vulnerability is 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.

An information disclosure vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the implementation of TLS protocol. Successful exploitation could allow an attacker to calculate the plaintext of secure connections.

#### 130014 - Debian Linux 7.0 DSA-3088-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8106

##### Description

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

DSA-3088-1

##### Observation

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

For more information see:

<http://www.debian.org/security/2014/dsa-3088>

Debian 7.0

all

qemu-kvm\_1.1.2+dfsg-6+deb7u6

#### 130017 - Debian Linux 7.0 DSA-3087-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8106

##### Description

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

DSA-3087-1

##### Observation

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

For more information see:

<http://www.debian.org/security/2014/dsa-3087>

Debian 7.0

all

qemu\_1.1.2+dfsg-6a+deb7u6

#### 142539 - SuSE SLES 11 SP3, SLED 11 SP3 pure-ftpd-10004 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:

pure-ftpd-10004

### Observation

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

<https://download.suse.com/Download?buildid=DZYTkuQAAIw~>  
<https://download.suse.com/Download?buildid=D34EHtdv6Rs~>  
<https://download.suse.com/Download?buildid=8btS1wsaw3s~>  
<https://download.suse.com/Download?buildid=n92wR9H8D2o~>  
<https://download.suse.com/Download?buildid=FYUjXSJwwyo~>  
[https://download.suse.com/Download?buildid=ia0jmFpCA\\_M~](https://download.suse.com/Download?buildid=ia0jmFpCA_M~)  
[https://download.suse.com/Download?buildid=\\_VyL07HPgVk~](https://download.suse.com/Download?buildid=_VyL07HPgVk~)  
<https://download.suse.com/Download?buildid=0j7zrf7PzqA~>  
<https://download.suse.com/Download?buildid=VKLCBNhsfGU~>

SuSE SLED 11 SP3  
x86\_64  
pure-ftpd-1.0.22-3.25.1

i586  
pure-ftpd-1.0.22-3.25.1

SuSE SLES 11 SP3  
x86\_64  
pure-ftpd-1.0.22-3.25.1

i586  
pure-ftpd-1.0.22-3.25.1

142557 - SuSE SLES 11 SP3, SLED 11 SP3 evolution-data-server-9969 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:  
evolution-data-server-9969

### Observation

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

<https://download.suse.com/Download?buildid=tUWCtbggqZQ~>  
<https://download.suse.com/Download?buildid=cGDqPoigJP4~>  
<https://download.suse.com/Download?buildid=1FIL5899oeg~>  
<https://download.suse.com/Download?buildid=AVdjpcUeLhI~>  
<https://download.suse.com/Download?buildid=c55UoLF18HY~>  
<https://download.suse.com/Download?buildid=wyX6G5yDI04~>  
<https://download.suse.com/Download?buildid=SA2GwUKil7g~>  
<https://download.suse.com/Download?buildid=S-rgRo0E5-0~>  
<https://download.suse.com/Download?buildid=OJi8XgvFNy4~>

SuSE SLED 11 SP3  
x86\_64  
evolution-data-server-2.28.2-0.32.1  
evolution-data-server-lang-2.28.2-0.32.1  
evolution-data-server-32bit-2.28.2-0.32.1

i586  
evolution-data-server-2.28.2-0.32.1  
evolution-data-server-lang-2.28.2-0.32.1

SuSE SLES 11 SP3  
x86\_64  
evolution-data-server-2.28.2-0.32.1  
evolution-data-server-lang-2.28.2-0.32.1  
evolution-data-server-32bit-2.28.2-0.32.1

i586  
evolution-data-server-2.28.2-0.32.1  
evolution-data-server-lang-2.28.2-0.32.1

174602 - Scientific Linux Security ERRATA Important: nss, nss-util, and nss-softokn on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-542)

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

Risk Level: Medium

CVE: CVE-2014-3566

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: nss, nss-util, and nss-softokn on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-542)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=542>

SL7  
x86\_64  
nss-sysinit-3.16.2.3-2.el7\_0  
nss-softokn-freebl-3.16.2.3-1.el7\_0  
nss-softokn-debuginfo-3.16.2.3-1.el7\_0  
nss-softokn-freebl-devel-3.16.2.3-1.el7\_0  
nss-pkcs11-devel-3.16.2.3-2.el7\_0  
nss-softokn-devel-3.16.2.3-1.el7\_0  
nss-devel-3.16.2.3-2.el7\_0  
nss-3.16.2.3-2.el7\_0  
nss-debuginfo-3.16.2.3-2.el7\_0  
nss-softokn-3.16.2.3-1.el7\_0  
nss-util-3.16.2.3-1.el7\_0  
nss-util-debuginfo-3.16.2.3-1.el7\_0  
nss-util-devel-3.16.2.3-1.el7\_0  
nss-tools-3.16.2.3-2.el7\_0

SL6  
x86\_64  
nss-pkcs11-devel-3.16.2.3-3.el6\_6  
nss-util-devel-3.16.2.3-2.el6\_6  
nss-3.16.2.3-3.el6\_6  
nss-sysinit-3.16.2.3-3.el6\_6  
nss-tools-3.16.2.3-3.el6\_6  
nss-util-3.16.2.3-2.el6\_6  
nss-debuginfo-3.16.2.3-3.el6\_6

nss-devel-3.16.2.3-3.el6\_6  
nss-util-debuginfo-3.16.2.3-2.el6\_6

i386

nss-pkcs11-devel-3.16.2.3-3.el6\_6  
nss-util-devel-3.16.2.3-2.el6\_6  
nss-3.16.2.3-3.el6\_6  
nss-sysinit-3.16.2.3-3.el6\_6  
nss-tools-3.16.2.3-3.el6\_6  
nss-util-3.16.2.3-2.el6\_6  
nss-debuginfo-3.16.2.3-3.el6\_6  
nss-devel-3.16.2.3-3.el6\_6  
nss-util-debuginfo-3.16.2.3-2.el6\_6

SL5

x86\_64  
nss-pkcs11-devel-3.16.2.3-1.el5\_11  
nss-tools-3.16.2.3-1.el5\_11  
nss-debuginfo-3.16.2.3-1.el5\_11  
nss-3.16.2.3-1.el5\_11  
nss-devel-3.16.2.3-1.el5\_11

i386

nss-pkcs11-devel-3.16.2.3-1.el5\_11  
nss-tools-3.16.2.3-1.el5\_11  
nss-debuginfo-3.16.2.3-1.el5\_11  
nss-3.16.2.3-1.el5\_11  
nss-devel-3.16.2.3-1.el5\_11

## 184634 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2436-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103

### Description

The scan detected that the host is missing the following update:  
USN-2436-1

### 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-December/002756.html>

Ubuntu 14.10

xserver-xorg-core\_1.16.0-1ubuntu1.1

Ubuntu 14.04

xserver-xorg-core\_1.15.1-0ubuntu2.4

Ubuntu 12.04

xserver-xorg-core\_1.11.4-0ubuntu10.15  
xserver-xorg-core-lts-trusty\_1.15.1-0ubuntu2-precise3

## 188591 - Fedora Linux 20 FEDORA-2014-15130 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8600

### Description

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

FEDORA-2014-15130

### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145229.html>

Fedora Core 20

kwebkitpart-1.3.4-5.fc20

## 188596 - Fedora Linux 21 FEDORA-2014-15150 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8600

### Description

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

FEDORA-2014-15150

### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145148.html>

Fedora Core 21

kwebkitpart-1.3.4-5.fc21

## 188597 - Fedora Linux 21 FEDORA-2014-15618 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8600

### Description

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

FEDORA-2014-15618

### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145155.html>

Fedora Core 21

kde-runtime-4.14.3-2.fc21

### 188601 - Fedora Linux 19 FEDORA-2014-15124 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8600

#### Description

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

FEDORA-2014-15124

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145724.html>

Fedora Core 19

kwebkitpart-1.3.4-5.fc19

### 88649 - Slackware Linux 14.1 SSA:2014-337-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

SSA:2014-337-01

#### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.359859>

Slackware 14.1

x86\_64

mozilla-thunderbird-31.3.0-x86\_64-1

### 130013 - Debian Linux 7.0 DSA-3092-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

#### Description



The scan detected that the host is missing the following update:  
DSA-3092-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3092>

Debian 7.0  
all  
icedove\_31.3.0-1~deb7u1

### 130016 - Debian Linux 7.0 DSA-3094-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8500

#### Description

The scan detected that the host is missing the following update:  
DSA-3094-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3094>

Debian 7.0  
all  
bind9\_1:9.8.4.dfsg.P1-6+nmu2+deb7u3

### 130018 - Debian Linux 7.0 DSA-3090-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

#### Description

The scan detected that the host is missing the following update:  
DSA-3090-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3090>

Debian 7.0  
all  
iceweasel\_31.3.0esr-1~deb7u1

### 142551 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1590-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8583

### Description

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

openSUSE-SU-2014:1590-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00036.html>

SuSE Linux 13.1

i586

apache2-mod\_wsgi-3.4-2.28.1

apache2-mod\_wsgi-debuginfo-3.4-2.28.1

apache2-mod\_wsgi-debugsource-3.4-2.28.1

SuSE Linux 12.3

i586

apache2-mod\_wsgi-debuginfo-3.3-12.8.1

apache2-mod\_wsgi-3.3-12.8.1

apache2-mod\_wsgi-debugsource-3.3-12.8.1

142555 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1581-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

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

openSUSE-SU-2014:1581-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00027.html>

SuSE Linux 13.1

x86\_64

libsoftokn3-debuginfo-32bit-3.17.2-47.2

mozilla-nss-sysinit-32bit-3.17.2-47.2

mozilla-nspr-32bit-4.10.7-19.1

mozilla-nss-debuginfo-32bit-3.17.2-47.2

mozilla-nspr-debuginfo-32bit-4.10.7-19.1

libfreebl3-32bit-3.17.2-47.2

libfreebl3-debuginfo-32bit-3.17.2-47.2

mozilla-nss-32bit-3.17.2-47.2

mozilla-nss-certs-32bit-3.17.2-47.2

mozilla-nss-sysinit-debuginfo-32bit-3.17.2-47.2

mozilla-nss-certs-debuginfo-32bit-3.17.2-47.2

libsoftokn3-32bit-3.17.2-47.2

i586

libfreebl3-3.17.2-47.2

MozillaFirefox-34.0.5-50.3

mozilla-nss-devel-3.17.2-47.2

MozillaFirefox-translations-common-34.0.5-50.3

libsoftokn3-debuginfo-3.17.2-47.2

mozilla-nss-certs-debuginfo-3.17.2-47.2

mozilla-nss-sysinit-debuginfo-3.17.2-47.2

mozilla-nspr-4.10.7-19.1

mozilla-nss-tools-debuginfo-3.17.2-47.2

mozilla-nss-certs-3.17.2-47.2

MozillaFirefox-debugsource-34.0.5-50.3

mozilla-nss-sysinit-3.17.2-47.2

mozilla-nspr-debugsource-4.10.7-19.1

mozilla-nss-tools-3.17.2-47.2

mozilla-nspr-debuginfo-4.10.7-19.1

MozillaFirefox-branding-upstream-34.0.5-50.3

MozillaFirefox-debuginfo-34.0.5-50.3

mozilla-nss-debugsource-3.17.2-47.2

libsoftokn3-3.17.2-47.2

MozillaFirefox-devel-34.0.5-50.3

mozilla-nss-debuginfo-3.17.2-47.2

MozillaFirefox-translations-other-34.0.5-50.3

mozilla-nss-3.17.2-47.2

mozilla-nspr-devel-4.10.7-19.1

MozillaFirefox-buildsymbols-34.0.5-50.3

libfreebl3-debuginfo-3.17.2-47.2

SuSE Linux 12.3

x86\_64

libsoftokn3-32bit-3.17.2-1.63.2

mozilla-nspr-32bit-4.10.7-1.37.1

libsoftokn3-debuginfo-32bit-3.17.2-1.63.2

mozilla-nss-32bit-3.17.2-1.63.2

mozilla-nss-certs-debuginfo-32bit-3.17.2-1.63.2

mozilla-nss-certs-32bit-3.17.2-1.63.2

mozilla-nspr-debuginfo-32bit-4.10.7-1.37.1

libfreebl3-32bit-3.17.2-1.63.2

mozilla-nss-debuginfo-32bit-3.17.2-1.63.2

libfreebl3-debuginfo-32bit-3.17.2-1.63.2

mozilla-nss-sysinit-32bit-3.17.2-1.63.2

mozilla-nss-sysinit-debuginfo-32bit-3.17.2-1.63.2

i586

mozilla-nss-certs-3.17.2-1.63.2

MozillaFirefox-branding-upstream-34.0.5-1.94.3

MozillaFirefox-34.0.5-1.94.3

libfreebl3-debuginfo-3.17.2-1.63.2

mozilla-nss-sysinit-3.17.2-1.63.2

libsoftokn3-debuginfo-3.17.2-1.63.2

libfreebl3-3.17.2-1.63.2

mozilla-nspr-4.10.7-1.37.1

mozilla-nss-sysinit-debuginfo-3.17.2-1.63.2

mozilla-nspr-debugsource-4.10.7-1.37.1

MozillaFirefox-buildsymbols-34.0.5-1.94.3

mozilla-nss-devel-3.17.2-1.63.2

MozillaFirefox-debugsource-34.0.5-1.94.3

mozilla-nss-3.17.2-1.63.2

MozillaFirefox-translations-other-34.0.5-1.94.3  
mozilla-nss-debugsource-3.17.2-1.63.2  
mozilla-nspr-devel-4.10.7-1.37.1  
mozilla-nss-certs-debuginfo-3.17.2-1.63.2  
mozilla-nspr-debuginfo-4.10.7-1.37.1  
MozillaFirefox-debuginfo-34.0.5-1.94.3  
mozilla-nss-tools-debuginfo-3.17.2-1.63.2  
mozilla-nss-debuginfo-3.17.2-1.63.2  
MozillaFirefox-translations-common-34.0.5-1.94.3  
libsoftokn3-3.17.2-1.63.2  
mozilla-nss-tools-3.17.2-1.63.2  
MozillaFirefox-devel-34.0.5-1.94.3

SuSE Linux 13.2

x86\_64

libfreebl3-32bit-3.17.2-4.2  
mozilla-nss-certs-debuginfo-32bit-3.17.2-4.2  
mozilla-nss-32bit-3.17.2-4.2  
libsoftokn3-32bit-3.17.2-4.2  
libsoftokn3-debuginfo-32bit-3.17.2-4.2  
libfreebl3-debuginfo-32bit-3.17.2-4.2  
mozilla-nspr-debuginfo-32bit-4.10.7-3.1  
mozilla-nss-sysinit-debuginfo-32bit-3.17.2-4.2  
mozilla-nss-sysinit-32bit-3.17.2-4.2  
mozilla-nss-certs-32bit-3.17.2-4.2  
mozilla-nss-debuginfo-32bit-3.17.2-4.2  
mozilla-nspr-32bit-4.10.7-3.1

i586

mozilla-nspr-devel-4.10.7-3.1  
mozilla-nss-tools-3.17.2-4.2  
mozilla-nss-certs-debuginfo-3.17.2-4.2  
MozillaFirefox-debugsource-34.0.5-5.4  
MozillaFirefox-translations-other-34.0.5-5.4  
libsoftokn3-3.17.2-4.2  
mozilla-nss-tools-debuginfo-3.17.2-4.2  
MozillaFirefox-buildsymbols-34.0.5-5.4  
mozilla-nss-sysinit-debuginfo-3.17.2-4.2  
MozillaFirefox-debuginfo-34.0.5-5.4  
mozilla-nss-certs-3.17.2-4.2  
mozilla-nss-sysinit-3.17.2-4.2  
MozillaFirefox-34.0.5-5.4  
MozillaFirefox-translations-common-34.0.5-5.4  
mozilla-nss-devel-3.17.2-4.2  
MozillaFirefox-branding-upstream-34.0.5-5.4  
mozilla-nss-debuginfo-3.17.2-4.2  
libfreebl3-debuginfo-3.17.2-4.2  
mozilla-nspr-4.10.7-3.1  
mozilla-nss-debugsource-3.17.2-4.2  
MozillaFirefox-devel-34.0.5-5.4  
libsoftokn3-debuginfo-3.17.2-4.2  
mozilla-nspr-debuginfo-4.10.7-3.1  
mozilla-nss-3.17.2-4.2  
mozilla-nspr-debugsource-4.10.7-3.1  
libfreebl3-3.17.2-4.2

177999 - Gentoo Linux GLSA-201412-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-1923

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-02

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-02.xml>

Affected packages:  
net-fs/nfs-utils < 1.2.8

181297 - FreeBSD unbound Can Be Tricked Into Following An Endless Series Of Delegations, This Consumes A Lot Of Resources (10d73529-7f4b-

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

Risk Level: Low

CVE: CVE-2014-8602

#### Description

The scan detected that the host is missing the following update:  
unbound -- can be tricked into following an endless series of delegations, this consumes a lot of resources (10d73529-7f4b-11e4-af66-00215af774f0)

#### Observation

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

<http://www.vuxml.org/freebsd/10d73529-7f4b-11e4-af66-00215af774f0.html>

Affected packages:  
unbound < 1.5.1

181299 - FreeBSD mozilla Multiple Vulnerabilities (7ae61870-9dd2-4884-a2f2-f19bb5784d09)

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

Risk Level: Low

CVE: CVE-2014-1569, CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

#### Description

The scan detected that the host is missing the following update:  
mozilla -- multiple vulnerabilities (7ae61870-9dd2-4884-a2f2-f19bb5784d09)

#### Observation

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

<http://www.vuxml.org/freebsd/7ae61870-9dd2-4884-a2f2-f19bb5784d09.html>

Affected packages:

firefox < 34.0.1  
firefox-esr < 31.3.0.1  
linux-firefox < 34.0.1  
linux-seamonkey < 2.31  
linux-thunderbird < 31.3.0  
seamonkey < 2.31  
thunderbird < 31.3.0  
libxul < 31.3.0  
nss < 3.17.3

#### 184635 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2428-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

#### Description

The scan detected that the host is missing the following update:  
USN-2428-1

#### 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-December/002749.html>

Ubuntu 14.10

thunderbird\_31.3.0+build1-0ubuntu0.14.10.1

Ubuntu 14.04

thunderbird\_31.3.0+build1-0ubuntu0.14.04.1

Ubuntu 12.04

thunderbird\_31.3.0+build1-0ubuntu0.12.04.1

#### 184637 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2431-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
USN-2431-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002752.html>

Ubuntu 14.10

maas-region-controller-min\_1.7.0~beta8+bzr3272-0ubuntu1.2

Ubuntu 14.04

maas-region-controller-min\_1.5.4+bzr2294-0ubuntu1.2

Ubuntu 12.04

maas-region-controller\_1.2+bzr1373+dfsg-0ubuntu1~12.04.6

#### 184638 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2431-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8583

#### Description

The scan detected that the host is missing the following update:  
USN-2431-1

#### 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-December/002748.html>

Ubuntu 14.10

libapache2-mod-wsgi-py3\_3.5-1ubuntu0.1

libapache2-mod-wsgi\_3.5-1ubuntu0.1

Ubuntu 14.04

libapache2-mod-wsgi-py3\_3.4-4ubuntu2.1.14.04.2

libapache2-mod-wsgi\_3.4-4ubuntu2.1.14.04.2

Ubuntu 12.04

libapache2-mod-wsgi\_3.3-4ubuntu0.2

libapache2-mod-wsgi-py3\_3.3-4ubuntu0.2

#### 184641 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2437-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8500

#### Description

The scan detected that the host is missing the following update:  
USN-2437-1

#### 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-December/002757.html>

Ubuntu 14.10

bind9\_9.9.5.dfsg-4.3ubuntu0.1

Ubuntu 14.04

bind9\_9.9.5.dfsg-3ubuntu0.1

Ubuntu 12.04

bind9\_9.8.1.dfsg.P1-4ubuntu0.9

Ubuntu 10.04

bind9\_9.7.0.dfsg.P1-1ubuntu0.12

### 188572 - Fedora Linux 21 FEDORA-2014-16162 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-2014-16162

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145324.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145323.html>

Fedora Core 21

thunderbird-31.3.0-1.fc21

firefox-34.0-1.fc21

### 188575 - Fedora Linux 19 FEDORA-2014-15733 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-2014-15733

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145172.html>

Fedora Core 19



## 188576 - Fedora Linux 21 FEDORA-2014-15968 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-2014-15968

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145632.html>

Fedora Core 21

libreoffice-4.3.4.1-8.fc21

## 188579 - Fedora Linux 21 FEDORA-2014-15776 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-2014-15776

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145707.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145699.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145706.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145698.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145697.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145702.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145696.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145694.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145704.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145695.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145700.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145705.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145703.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145701.html>

Fedora Core 21

jenkins-matrix-project-plugin-1.4-1.fc21

jenkins-mailer-plugin-1.12-1.fc21

jenkins-ssh-credentials-plugin-1.10-3.fc21  
jenkins-winstone-2.8-1.fc21  
jenkins-remoting-2.48-1.fc21  
jenkins-ant-plugin-1.2-3.fc21  
jenkins-credentials-plugin-1.18-2.fc21  
jenkins-icon-shim-1.0.4-1.fc21  
stapler-1.233-1.fc21  
jenkins-1.590-1.fc21  
jenkins-external-monitor-job-plugin-1.4-1.fc21  
jenkins-junit-plugin-1.2-1.fc21  
jenkins-ssh-slaves-plugin-1.9-2.fc21  
jenkins-javadoc-plugin-1.3-1.fc21

## 188580 - Fedora Linux 21 FEDORA-2014-15862 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-2014-15862

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145644.html>

Fedora Core 21

hexchat-2.10.2-1.fc21

## 188582 - Fedora Linux 21 FEDORA-2014-15779 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-6407, CVE-2014-6408

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15779

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145154.html>

Fedora Core 21

docker-io-1.3.2-2.fc21

## 188584 - Fedora Linux 21 FEDORA-2014-15670 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-2014-15670

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145650.html>

Fedora Core 21

teeworlds-0.6.3-1.fc21

### 188586 - Fedora Linux 21 FEDORA-2014-15143 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-2014-15143

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145428.html>

Fedora Core 21

moodle-2.7.3-1.fc21

### 188587 - Fedora Linux 21 FEDORA-2014-15586 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-2014-15586

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145443.html>

Fedora Core 21

mod\_wsgi-4.3.2-1.fc21

### 188589 - Fedora Linux 20 FEDORA-2014-15701 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-2014-15701

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145173.html>

Fedora Core 20

teeworlds-0.6.3-1.fc20

### 188590 - Fedora Linux 19 FEDORA-2014-15833 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-2014-15833

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145741.html>

Fedora Core 19

hivex-1.3.8-2.fc19

### 188592 - Fedora Linux 19 FEDORA-2014-16242 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-2014-16242

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145730.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145729.html>

Fedora Core 19

thunderbird-31.3.0-1.fc19  
firefox-34.0-1.fc19

### 188594 - Fedora Linux 21 FEDORA-2014-15748 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-2014-15748

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145358.html>

Fedora Core 21

hivex-1.3.11-4.fc21

### 188602 - Fedora Linux 21 FEDORA-2014-15450 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1934

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15450

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145388.html>

Fedora Core 21

python-eyed3-0.7.4-4.fc21

### 188607 - Fedora Linux 19 FEDORA-2014-7496 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-2014-7496

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145720.html>

Fedora Core 19

readline-6.2-8.fc19

### 188608 - Fedora Linux 20 FEDORA-2014-15841 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-2014-15841

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145242.html>

Fedora Core 20

hivex-1.3.8-4.fc20

### 188609 - Fedora Linux 20 FEDORA-2014-16016 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9114

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16016

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145188.html>

Fedora Core 20

util-linux-2.24.2-2.fc20

## 188612 - Fedora Linux 20 FEDORA-2014-16259 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-2014-16259

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145198.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145199.html>

Fedora Core 20

firefox-34.0-1.fc20

thunderbird-31.3.0-1.fc20

## 85835 - CentOS 5 CESA-2014-1959 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-0181

### Description

The scan detected that the host is missing the following update:  
CESA-2014-1959

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020806.html>

CentOS 5

x86\_64

kernel-xen-devel-2.6.18-400.el5

kernel-debug-devel-2.6.18-400.el5

kernel-debug-2.6.18-400.el5

kernel-devel-2.6.18-400.el5

kernel-2.6.18-400.el5

kernel-headers-2.6.18-400.el5

kernel-xen-2.6.18-400.el5

i686

kernel-2.6.18-400.el5

kernel-devel-2.6.18-400.el5

kernel-xen-2.6.18-400.el5

kernel-xen-devel-2.6.18-400.el5

kernel-debug-2.6.18-400.el5  
kernel-PAE-devel-2.6.18-400.el5  
kernel-PAE-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.el5

i386  
kernel-headers-2.6.18-400.el5

noarch  
kernel-doc-2.6.18-400.el5

## 91682 - Oracle Enterprise Linux ELSA-2014-1959 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-0181

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1959

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004696.html>  
<http://oss.oracle.com/pipermail/el-errata/2014-December/004692.html>

OEL5  
x86\_64  
kernel-headers-2.6.18-400.0.0.0.1.el5  
kernel-2.6.18-400.el5  
kernel-devel-2.6.18-400.el5  
kernel-xen-2.6.18-400.0.0.0.1.el5  
kernel-xen-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.0.0.0.1.el5  
kernel-headers-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.0.0.0.1.el5  
kernel-xen-devel-2.6.18-400.el5  
kernel-devel-2.6.18-400.0.0.0.1.el5  
kernel-debug-2.6.18-400.el5  
kernel-2.6.18-400.0.0.0.1.el5  
kernel-debug-2.6.18-400.0.0.0.1.el5  
kernel-doc-2.6.18-400.0.0.0.1.el5  
kernel-doc-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.el5

i386  
kernel-xen-2.6.18-400.el5  
kernel-debug-2.6.18-400.el5  
kernel-2.6.18-400.el5  
kernel-xen-2.6.18-400.0.0.0.1.el5  
kernel-doc-2.6.18-400.el5  
kernel-headers-2.6.18-400.0.0.0.1.el5  
kernel-devel-2.6.18-400.el5  
kernel-devel-2.6.18-400.0.0.0.1.el5  
kernel-doc-2.6.18-400.0.0.0.1.el5  
kernel-debug-2.6.18-400.0.0.0.1.el5



kernel-debug-devel-2.6.18-400.0.0.1.el5  
kernel-headers-2.6.18-400.el5  
kernel-2.6.18-400.0.0.1.el5  
kernel-debug-devel-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.0.0.1.el5  
kernel-PAE-devel-2.6.18-400.0.0.1.el5  
kernel-PAE-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.el5  
kernel-PAE-2.6.18-400.0.0.1.el5  
kernel-PAE-devel-2.6.18-400.el5

## 140632 - Red Hat Enterprise Linux RHSA-2014-1959 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-0181

### Description

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

RHSA-2014-1959

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2014-1959.html>

### RHEL5D

x86\_64

kernel-xen-debuginfo-2.6.18-400.el5  
kernel-2.6.18-400.el5  
kernel-debuginfo-common-2.6.18-400.el5  
kernel-debug-debuginfo-2.6.18-400.el5  
kernel-headers-2.6.18-400.el5  
kernel-devel-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.el5  
kernel-debuginfo-2.6.18-400.el5  
kernel-debug-2.6.18-400.el5  
kernel-xen-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.el5

i386

kernel-xen-debuginfo-2.6.18-400.el5  
kernel-PAE-debuginfo-2.6.18-400.el5  
kernel-2.6.18-400.el5  
kernel-devel-2.6.18-400.el5  
kernel-debuginfo-common-2.6.18-400.el5  
kernel-headers-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.el5  
kernel-debug-debuginfo-2.6.18-400.el5  
kernel-debug-2.6.18-400.el5  
kernel-PAE-devel-2.6.18-400.el5  
kernel-debuginfo-2.6.18-400.el5  
kernel-xen-2.6.18-400.el5  
kernel-PAE-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.el5

noarch

kernel-doc-2.6.18-400.el5

RHEL5S

x86\_64

kernel-xen-debuginfo-2.6.18-400.el5

kernel-2.6.18-400.el5

kernel-debuginfo-common-2.6.18-400.el5

kernel-debug-debuginfo-2.6.18-400.el5

kernel-headers-2.6.18-400.el5

kernel-devel-2.6.18-400.el5

kernel-xen-devel-2.6.18-400.el5

kernel-debuginfo-2.6.18-400.el5

kernel-debug-2.6.18-400.el5

kernel-xen-2.6.18-400.el5

kernel-debug-devel-2.6.18-400.el5

i386

kernel-xen-debuginfo-2.6.18-400.el5

kernel-PAE-debuginfo-2.6.18-400.el5

kernel-2.6.18-400.el5

kernel-devel-2.6.18-400.el5

kernel-debuginfo-common-2.6.18-400.el5

kernel-headers-2.6.18-400.el5

kernel-xen-devel-2.6.18-400.el5

kernel-debug-debuginfo-2.6.18-400.el5

kernel-debug-2.6.18-400.el5

kernel-PAE-devel-2.6.18-400.el5

kernel-debuginfo-2.6.18-400.el5

kernel-xen-2.6.18-400.el5

kernel-PAE-2.6.18-400.el5

kernel-debug-devel-2.6.18-400.el5

noarch

kernel-doc-2.6.18-400.el5

## 170433 - Amazon Linux AMI ALAS-2014-457 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-6497

### Description

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

ALAS-2014-457

### Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2014-457.html>

Amazon Linux AMI

x86\_64

clamav-0.98.5-1.10.amzn1

clamav-milter-0.98.5-1.10.amzn1

clamav-update-0.98.5-1.10.amzn1

clamav-devel-0.98.5-1.10.amzn1

clamav-lib-0.98.5-1.10.amzn1

clamav-server-0.98.5-1.10.amzn1  
clamav-db-0.98.5-1.10.amzn1  
clamd-0.98.5-1.10.amzn1  
clamav-debuginfo-0.98.5-1.10.amzn1

i686

clamav-0.98.5-1.10.amzn1  
clamav-milter-0.98.5-1.10.amzn1  
clamav-lib-0.98.5-1.10.amzn1  
clamav-update-0.98.5-1.10.amzn1  
clamav-devel-0.98.5-1.10.amzn1  
clamd-0.98.5-1.10.amzn1  
clamav-server-0.98.5-1.10.amzn1  
clamav-db-0.98.5-1.10.amzn1  
clamav-debuginfo-0.98.5-1.10.amzn1

noarch

clamav-data-0.98.5-1.10.amzn1  
clamav-filesystem-0.98.5-1.10.amzn1  
clamav-scanner-0.98.5-1.10.amzn1  
clamav-data-empty-0.98.5-1.10.amzn1  
clamav-server-sysvinit-0.98.5-1.10.amzn1  
clamav-scanner-sysvinit-0.98.5-1.10.amzn1  
clamav-milter-sysvinit-0.98.5-1.10.amzn1

174603 - Scientific Linux Security ERRATA Moderate: kernel on SL5.x i386/x86\_64 (1412-1102)

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

Risk Level: Low

CVE: CVE-2014-0181

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Moderate: kernel on SL5.x i386/x86\_64 (1412-1102)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=1102>

SL5

x86\_64

kernel-xen-debuginfo-2.6.18-400.el5  
kernel-2.6.18-400.el5  
kernel-debuginfo-common-2.6.18-400.el5  
kernel-debug-debuginfo-2.6.18-400.el5  
kernel-headers-2.6.18-400.el5  
kernel-devel-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.el5  
kernel-debuginfo-2.6.18-400.el5  
kernel-debug-2.6.18-400.el5  
kernel-xen-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.el5

i386

kernel-xen-debuginfo-2.6.18-400.el5  
kernel-PAE-debuginfo-2.6.18-400.el5

kernel-2.6.18-400.el5  
kernel-devel-2.6.18-400.el5  
kernel-debuginfo-common-2.6.18-400.el5  
kernel-headers-2.6.18-400.el5  
kernel-xen-devel-2.6.18-400.el5  
kernel-debug-debuginfo-2.6.18-400.el5  
kernel-debug-2.6.18-400.el5  
kernel-PAE-devel-2.6.18-400.el5  
kernel-debuginfo-2.6.18-400.el5  
kernel-xen-2.6.18-400.el5  
kernel-PAE-2.6.18-400.el5  
kernel-debug-devel-2.6.18-400.el5

noarch  
kernel-doc-2.6.18-400.el5

#### 43154 - HP-UX 11.X PHSS\_44173 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
PHSS\_44173

#### Observation

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

[https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHSS\\_44173](https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHSS_44173)

">patch description</a>

HP-UX 11.31 (NA)

DCE-Core.DCE-IA64-SHLIB,fr=B.11.31,fa=HP-UX\_B.11.31\_IA,v=HP  
DCE-Core.DCE-CORE-SHLIB,fr=B.11.31,fa=HP-UX\_B.11.31\_IA,v=HP  
DCE-Core.DCE-COR-64SLIB,fr=B.11.31,fa=HP-UX\_B.11.31\_PA,v=HP  
DCE-Core.DCEC-ENG-A-MAN,fr=B.11.31,fa=HP-UX\_B.11.31\_IA/PA,v=HP  
DCE-Core.DCE-CORE-SHLIB,fr=B.11.31,fa=HP-UX\_B.11.31\_PA,v=HP  
DCE-Core.DCE-CORE-RUN,fr=B.11.31,fa=HP-UX\_B.11.31\_PA,v=HP  
DCE-Core.DCE-CORE-RUN,fr=B.11.31,fa=HP-UX\_B.11.31\_IA,v=HP  
DCE-Core.DCE-CORE-DTS,fr=B.11.31,fa=HP-UX\_B.11.31\_PA,v=HP  
DCE-Core.DCE-COR-64SLIB,fr=B.11.31,fa=HP-UX\_B.11.31\_IA,v=HP  
DCE-Core.DCE-CORE-DTS,fr=B.11.31,fa=HP-UX\_B.11.31\_IA,v=HP

#### 43155 - HP-UX 11.X PHCO\_44147 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
PHCO\_44147

## Observation

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

For more information see:

[https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHCO\\_44147](https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHCO_44147)

">patch description</a>

HP-UX 11.11 (800)

HP-UX 11.11 (700)

PrinterMgmt.LPSP-ENG-A-MAN,fr=B.11.11,fa=HP-UX\_B.11.11\_32/64,v=HP

PrinterMgmt.LP-SPOOL,fr=B.11.11,fa=HP-UX\_B.11.11\_32/64,v=HP

## 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.

### 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

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

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

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

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

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

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

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: High

CVE: CVE-2014-1804

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

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

17485 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow (3017301)

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

Risk Level: High



CVE: CVE-2014-6356 , CVE-2014-6357

Update Details

Recommendation is updated FASLScript is updated

17486 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow (3017301)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6356 , CVE-2014-6357

Update Details

Recommendation is updated

17487 - (MS14-083) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (3017347)

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

Risk Level: High

CVE: CVE-2014-6360 , CVE-2014-6361

Update Details

Recommendation is updated

2131 - W32/Mydoom@MM Server Detected

Category: General Vulnerability Assessment -> NonIntrusive -> Trojan, Backdoors, Viruses, and Malware

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript 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

#### 4360 - (MS06-013) Microsoft Internet Explorer HTA Execution Vulnerability

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

Risk Level: High

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

[Update Details](#)

Recommendation is updated

#### 4412 - (MS06-024) Microsoft Windows Media Player Vulnerability (917734)

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

Risk Level: High

CVE: CVE-2006-0025

[Update Details](#)

Recommendation is updated

#### 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

#### 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

### 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

#### 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

#### 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

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

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

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

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

#### 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

---

### 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

**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

**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

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

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

## 6110 - (MS08-053) Microsoft Windows Media Encoder Remote Code Execution (954156)

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

Risk Level: High

CVE: CVE-2008-3008

### Update Details

Recommendation is updated

## 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

6273 - (MS08-071) Microsoft GDI Heap Overflow Vulnerability (956802)

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

Risk Level: High

CVE: CVE-2008-3465

Update Details

Recommendation is updated

6274 - (MS08-071) Microsoft GDI Integer Overflow Vulnerability (956802)

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

Risk Level: High

CVE: CVE-2008-2249

Update Details

Recommendation is updated

6283 - (MS08-073) Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerability (958215)

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

Risk Level: High

CVE: CVE-2008-4259

Update Details

Recommendation is updated

6284 - (MS08-073) Microsoft Internet Explorer HTML Rendering Memory Corruption Vulnerability (958215)

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

Risk Level: High

CVE: CVE-2008-4261

Update Details

Recommendation is updated

6287 - (MS08-074) Microsoft Excel File Format Parsing Vulnerability I (959070)



---

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

Risk Level: High

CVE: CVE-2008-4265

Update Details

Recommendation is updated

6288 - (MS08-074) Microsoft Excel File Format Parsing Vulnerability II (959070)

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

Risk Level: High

CVE: CVE-2008-4264

Update Details

Recommendation is updated

6289 - (MS08-074) Microsoft Excel Global Array Memory Corruption Vulnerability (959070)

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

Risk Level: High

CVE: CVE-2008-4266

Update Details

Recommendation is updated

6315 - (MS09-004) Microsoft SQL Server sp\_replwritetovarbin Limited Memory Overwrite Vulnerability (959420)

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

Risk Level: High

CVE: CVE-2008-5416

Update Details

Recommendation is updated

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

6759 - (MS09-021) Microsoft Office Excel Record Pointer Corruption Vulnerability II (969462)

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

Risk Level: High

CVE: CVE-2009-1134

[Update Details](#)

Recommendation is updated

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

7206 - (MS09-060) ATL COM Initialization Vulnerability (973965)

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

Risk Level: High

CVE: CVE-2009-2493

[Update Details](#)

Recommendation is updated

7207 - (MS09-060) ATL Uninitialized Object Vulnerability (973965)

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

Risk Level: High

CVE: CVE-2009-0901

[Update Details](#)

Recommendation is updated

7211 - (MS09-062) GDI+ .Net PropertyItem Heap Overflow Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2504

[Update Details](#)

Recommendation is updated

#### 7212 - (MS09-062) GDI+ PNG Heap Overflow Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2501

[Update Details](#)

Recommendation is updated

#### 7213 - (MS09-062) GDI+ PNG Integer Overflow Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-3126

[Update Details](#)

Recommendation is updated

#### 7214 - (MS09-062) GDI+ TIFF Memory Corruption Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2503

[Update Details](#)

Recommendation is updated

#### 7215 - (MS09-062) GDI+ TIFF Buffer Overflow Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2502

[Update Details](#)

Recommendation is updated

#### 7216 - (MS09-062) GDI+ WMF Integer Overflow Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2500

[Update Details](#)

Recommendation is updated

---

## 7217 - (MS09-062) Memory Corruption Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2528

### Update Details

Recommendation is updated

## 7218 - (MS09-062) Office BMP Integer Overflow Vulnerability (957488)

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

Risk Level: High

CVE: CVE-2009-2518

### Update Details

Recommendation is updated

## 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

## 7319 - (MS09-067) Excel Cache Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3127

### Update Details

Recommendation is updated

## 7320 - (MS09-067) Excel SxView Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3128

### Update Details

Recommendation is updated

## 7321 - (MS09-067) Excel Featherer Record Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3129

Update Details

Recommendation is updated

7322 - (MS09-067) Excel Document Parsing Heap Overflow Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3130

Update Details

Recommendation is updated

7323 - (MS09-067) Excel Formula Parsing Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3131

Update Details

Recommendation is updated

7324 - (MS09-067) Excel Index Parsing Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3132

Update Details

Recommendation is updated

7325 - (MS09-067) Excel Document Parsing Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3133

Update Details

Recommendation is updated

7326 - (MS09-067) Excel Field Sanitization Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3134

Update Details

Recommendation is updated

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

7366 - (MS09-004) Vulnerability In Microsoft SQL Server Could Allow Remote Code Execution (959420)

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

Risk Level: High

CVE: CVE-2008-5416

Update Details

Recommendation is updated

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

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

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

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

7706 - (MS08-053) Vulnerability In Windows Media Encoder 9 Could Allow Remote Code Execution (954156)

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

Risk Level: High

CVE: CVE-2008-3008

Update Details

Recommendation is updated

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

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

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

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

## 8106 - (MS10-017) Microsoft Office Excel Record Memory Corruption Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0257

### Update Details

Recommendation is updated

## 8107 - (MS10-017) Microsoft Office Excel Sheet Object Type Confusion Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0258

### Update Details

Recommendation is updated

## 8108 - (MS10-017) Microsoft Office Excel MDXTUPLE Record Heap Overflow Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0260

### Update Details

Recommendation is updated

## 8109 - (MS10-017) Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0261

### Update Details

Recommendation is updated

## 8110 - (MS10-017) Microsoft Office Excel FNGROUPNAME Record Uninitialized Memory Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0262

### Update Details

Recommendation is updated

---

## 8111 - (MS10-017) Microsoft Office Excel XLSX File Parsing Code Execution Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0263

### Update Details

Recommendation is updated

## 8112 - (MS10-017) Microsoft Office Excel DbOrParamQry Record Parsing Vulnerability (980150)

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

Risk Level: High

CVE: CVE-2010-0264

### Update Details

Recommendation is updated

## 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

## 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

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

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

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

9088 - (MS10-038) Microsoft Office Excel Record Parsing Memory Corruption Vulnerability (2027452)

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

Risk Level: High

CVE: CVE-2010-0821

Update Details

Recommendation is updated

9089 - (MS10-038) Microsoft Office Excel Object Stack Overflow Vulnerability (2027452)

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

Risk Level: High

CVE: CVE-2010-0822

Update Details

Recommendation is updated

9090 - (MS10-038) Microsoft Office Excel Memory Corruption Vulnerability (2027452)

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

Risk Level: High

CVE: CVE-2010-0823

Update Details

Recommendation is updated

9091 - (MS10-038) Microsoft Office Excel Record Memory Corruption Vulnerability (2027452)

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

Risk Level: High

CVE: CVE-2010-0824

Update Details

Recommendation is updated

9092 - (MS10-038) Microsoft Office Excel Record Memory Corruption Vulnerability (2027452) CVE-2010-1245

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

Risk Level: High

CVE: CVE-2010-1245

Update Details

Recommendation is updated

9093 - (MS10-038) Microsoft Office Excel RTD Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1246

[Update Details](#)

Recommendation is updated

#### 9094 - (MS10-038) Microsoft Excel Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1247

[Update Details](#)

Recommendation is updated

#### 9095 - (MS10-038) Microsoft Excel HFPicture Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1248

[Update Details](#)

Recommendation is updated

#### 9096 - (MS10-038) Microsoft Excel Memory Corruption Vulnerability II (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1249

[Update Details](#)

Recommendation is updated

#### 9097 - (MS10-038) Microsoft Excel EDG Memory Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1250

[Update Details](#)

Recommendation is updated

#### 9098 - (MS10-038) Microsoft Excel Record Stack Corruption Vulnerability (2027452)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High



CVE: CVE-2010-1251

[Update Details](#)

Recommendation is updated

9099 - (MS10-038) Microsoft Excel String Variable Vulnerability (2027452)

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

Risk Level: High

CVE: CVE-2010-1252

[Update Details](#)

Recommendation is updated

9100 - (MS10-038) Microsoft Excel ADO Object Vulnerability (2027452)

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

Risk Level: High

CVE: CVE-2010-1253

[Update Details](#)

Recommendation is updated

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

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

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

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

10357 - (MS10-080) Microsoft Office Excel Record Parsing Integer Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3230

Update Details

Recommendation is updated

10359 - (MS10-080) Microsoft Office Excel Record Parsing Memory Corruption (2293211)

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

Risk Level: High

CVE: CVE-2010-3231

Update Details

Recommendation is updated

10367 - (MS10-080) Microsoft Office Excel File Format Parsing Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3232

Update Details

Recommendation is updated

10368 - (MS10-080) Microsoft Office Lotus 1-2-3 Workbook Parsing Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3233

Update Details

Recommendation is updated

10369 - (MS10-080) Microsoft Office Formula Substream Memory Corruption (2293211)

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

Risk Level: High

CVE: CVE-2010-3234

Update Details

Recommendation is updated

10370 - (MS10-080) Microsoft Office Formula Biff Record Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3235

Update Details

Recommendation is updated

10373 - (MS10-080) Microsoft Office Out Of Bounds Array Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3236

Update Details

Recommendation is updated

10374 - (MS10-080) Microsoft Office Merge Cell Record Pointer Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3237

Update Details

Recommendation is updated

10375 - (MS10-080) Microsoft Office Negative Future Function Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3238

Update Details

Recommendation is updated

10379 - (MS10-080) Microsoft Office Extra Out of Boundary Record Parsing Remote Code Execution (2293211)

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

Risk Level: High

CVE: CVE-2010-3239

Update Details

Recommendation is updated

10380 - (MS10-080) Microsoft Office Real Time Data Array Record Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes



(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3240

[Update Details](#)

Recommendation is updated

### 10381 - (MS10-080) Microsoft Office Out-of-Bounds Memory Write in Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3241

[Update Details](#)

Recommendation is updated

### 10382 - (MS10-080) Microsoft Office Ghost Record Type Parsing Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3242

[Update Details](#)

Recommendation is updated

### 10383 - (MS10-080) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3230, CVE-2010-3231, CVE-2010-3232, CVE-2010-3233, CVE-2010-3234, CVE-2010-3235, CVE-2010-3236, CVE-2010-3237, CVE-2010-3238, CVE-2010-3239, CVE-2010-3240, CVE-2010-3241, CVE-2010-3242

[Update Details](#)

Recommendation is updated

### 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

### 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

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

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

#### 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

#### 11340 - (MS11-022) Microsoft PowerPoint OfficeArt Atom RCE (2489283)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0976

[Update Details](#)

Recommendation is updated

#### 11342 - (MS11-021) Microsoft Excel Array Indexing (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0978

[Update Details](#)

Recommendation is updated

#### 11343 - (MS11-021) Microsoft Excel Linked List Corruption (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0979

[Update Details](#)

Recommendation is updated

#### 11344 - (MS11-021) Microsoft Excel Dangling Pointer (2489279)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0980

[Update Details](#)

Recommendation is updated

#### 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

11775 - (MS11-021) Microsoft Excel Integer Overrun (2489279)

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

Risk Level: High

CVE: CVE-2011-0097

Update Details

Recommendation is updated

11777 - (MS11-021) Microsoft Excel Record Parsing WriteAV (2489279)

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

Risk Level: High

CVE: CVE-2011-0101

Update Details

Recommendation is updated

11778 - (MS11-021) Microsoft Excel Memory Corruption (2489279)

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

Risk Level: High

CVE: CVE-2011-0103

Update Details

Recommendation is updated

11779 - (MS11-021) Microsoft Excel Heap Overflow (2489279)

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

Risk Level: High

CVE: CVE-2011-0098

Update Details

Recommendation is updated

11780 - (MS11-021) Microsoft Excel Buffer Overwrite (2489279)

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

Risk Level: High

CVE: CVE-2011-0104

Update Details

Recommendation is updated

11781 - (MS11-021) Microsoft Excel Data Initialization (2489279)

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

Risk Level: High

CVE: CVE-2011-0105

Update Details

Recommendation is updated

11782 - (MS11-022) Microsoft PowerPoint Floating Point Techno-color Time Bandit RCE (2489283)

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

Risk Level: High

CVE: CVE-2011-0655

Update Details

Recommendation is updated

11783 - (MS11-022) Microsoft PowerPoint Persist Directory RCE (2489283)

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

Risk Level: High

CVE: CVE-2011-0656

Update Details

Recommendation is updated

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

12208 - (MS11-045) Microsoft Excel Buffer Overrun Remote Code Execution (2537146)

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

Risk Level: High

CVE: CVE-2011-1276

Update Details

Recommendation is updated

12209 - (MS11-045) Microsoft Excel Improper Record Parsing Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1273

Update Details

Recommendation is updated

## 12210 - (MS11-045) Microsoft Excel Insufficient Record Validation Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1272

### Update Details

Recommendation is updated

## 12213 - (MS11-045) Microsoft Excel Memory Heap Overwrite Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1275

### Update Details

Recommendation is updated

## 12214 - (MS11-045) Microsoft Excel Out of Bounds Array Access Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1274

### Update Details

Recommendation is updated

## 12215 - (MS11-050) Cumulative Security Update for Internet Explorer (2530548)

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

Risk Level: High

CVE: CVE-2011-1246, CVE-2011-1250, CVE-2011-1251, CVE-2011-1252, CVE-2011-1254, CVE-2011-1255, CVE-2011-1256, CVE-2011-1258, CVE-2011-1260, CVE-2011-1261, CVE-2011-1262

### Update Details

Recommendation is updated

## 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

#### 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

12616 - (MS11-072) Microsoft Excel Conditional Expression Parsing Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1989

Update Details

Recommendation is updated

12617 - (MS11-072) Microsoft Excel Heap Corruption Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1988

Update Details

Recommendation is updated

12618 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1987

[Update Details](#)

Recommendation is updated

#### 12619 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution II (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1990

[Update Details](#)

Recommendation is updated

#### 12620 - (MS11-072) Microsoft Excel Use after Free WriteAV Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1986

[Update Details](#)

Recommendation is updated

#### 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

#### 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

#### 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

13057 - (MS11-089) Microsoft Word Access Violation (2590602)

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

Risk Level: High

CVE: CVE-2011-1983

Update Details

Recommendation is updated

13061 - (MS11-089) Vulnerabilities in Microsoft Word could allow for Remote Code Execution (2590602)

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

Risk Level: High

CVE: CVE-2011-1983

Update Details

Recommendation is updated

13064 - (MS11-099) Microsoft Internet Explorer Insecure Library Loading (2618444)

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

Risk Level: High

CVE: CVE-2011-2019

Update Details

Recommendation is updated

### 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

### 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

### 13505 - (MS12-027) Microsoft Office And SQL Server MSCOMCTL.OCX Remote Code Execution (2664258)

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

Risk Level: High

CVE: CVE-2012-0158

#### Update Details

Recommendation is updated

### 13506 - (MS12-027) Vulnerability In Windows Common Controls Could Allow Remote Code Execution (2664258)

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

Risk Level: High

CVE: CVE-2012-0158

#### Update Details

Recommendation is updated

### 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

### 13606 - (MS12-030) Microsoft Office Excel Record Parsting Type Mismatch Remote Code Execution



(2663830)

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

Risk Level: High

CVE: CVE-2012-1847

[Update Details](#)

Recommendation is updated

13607 - (MS12-030) Microsoft Office Excel MergeCells Heap Overflow Remote Code Execution (2663830)

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

Risk Level: High

CVE: CVE-2012-0185

[Update Details](#)

Recommendation is updated

13608 - (MS12-030) Microsoft Office Excel SXLI Record Memory Corruption Remote Code Execution (2663830)

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

Risk Level: High

CVE: CVE-2012-0184

[Update Details](#)

Recommendation is updated

13609 - (MS12-030) Microsoft Office Excel Memory Corruption Using Various Modified Bytes (2663830)

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

Risk Level: High

CVE: CVE-2012-0143

[Update Details](#)

Recommendation is updated

13610 - (MS12-030) Microsoft Office Excel File Format Memory Corruption in OBJECTLINK Record (2663830)

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

Risk Level: High

CVE: CVE-2012-0142

[Update Details](#)

Recommendation is updated

### 13611 - (MS12-030) Microsoft Office Excel File Format Memory Corruption (2663830)

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

Risk Level: High

CVE: CVE-2012-0141

#### Update Details

Recommendation is updated

### 13612 - (MS12-030) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2663830)

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

Risk Level: High

CVE: CVE-2012-0141, CVE-2012-0142, CVE-2012-0143, CVE-2012-0184, CVE-2012-0185, CVE-2012-1847

#### Update Details

Recommendation is updated

### 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

### 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

### 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

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

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

14355 - (MS12-076) Microsoft Excel SerAuxErrBar Remote Code Execution (2720184)

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

Risk Level: High

CVE: CVE-2012-1885

Update Details

Recommendation is updated

14356 - (MS12-076) Microsoft Excel Memory Corruption Remote Code Execution (2720184)

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

Risk Level: High

CVE: CVE-2012-1886

Update Details

Recommendation is updated

14357 - (MS12-076) Microsoft Excel SST Invalid Length Remote Code Execution (2720184)

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

Risk Level: High

CVE: CVE-2012-1887

[Update Details](#)

Recommendation is updated

14358 - (MS12-076) Microsoft Excel Stack Overflow Remote Code Execution (2720184)

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

Risk Level: High

CVE: CVE-2012-2543

[Update Details](#)

Recommendation is updated

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

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

#### 14759 - MariaDB Multiple Vulnerabilities Prior To 5.5.29

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

Risk Level: High

CVE: CVE-2012-0572, CVE-2012-0574, CVE-2012-0578, CVE-2012-1702, CVE-2012-1705, CVE-2012-5060, CVE-2012-5096, CVE-2012-5611, CVE-2012-5612, CVE-2012-5615, CVE-2012-5627, CVE-2013-0367, CVE-2013-0368, CVE-2013-0371, CVE-2013-0375, CVE-2013-0383, CVE-2013-0384, CVE-2013-0385, CVE-2013-0386, CVE-2013-0389

[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

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

#### 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

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

#### 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

15389 - (MS13-059) Cumulative Security Update for Internet Explorer (2862772)

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



Risk Level: High

CVE: CVE-2013-3184, CVE-2013-3186, CVE-2013-3187, CVE-2013-3188, CVE-2013-3189, CVE-2013-3190, CVE-2013-3191, CVE-2013-3192, CVE-2013-3193, CVE-2013-3194, CVE-2013-3199

Update Details

Recommendation is updated

15531 - (MS13-073) Vulnerabilities In Microsoft Excel Could Allow Remote Code Execution (2858300)

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

Risk Level: High

CVE: CVE-2013-1315, CVE-2013-3158, CVE-2013-3159

Update Details

Recommendation is updated

15534 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution I (2858300)

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

Risk Level: High

CVE: CVE-2013-1315

Update Details

Recommendation is updated

15535 - (MS13-072) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2845537)

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

Risk Level: High

CVE: CVE-2013-3160, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3850, CVE-2013-3851, CVE-2013-3852, CVE-2013-3853, CVE-2013-3854, CVE-2013-3855, CVE-2013-3856, CVE-2013-3857, CVE-2013-3858

Update Details

Recommendation is updated

15537 - (MS13-069) Cumulative Security Update for Internet Explorer (2870699)

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

Risk Level: High

CVE: CVE-2013-3201, CVE-2013-3202, CVE-2013-3203, CVE-2013-3204, CVE-2013-3205, CVE-2013-3206, CVE-2013-3207, CVE-2013-3208, CVE-2013-3209, CVE-2013-3845

Update Details

Recommendation is updated

15540 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution I (2870699)

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

Risk Level: High

CVE: CVE-2013-3201

Update Details

Recommendation is updated

15545 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution II (2870699)

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

Risk Level: High

CVE: CVE-2013-3202

Update Details

Recommendation is updated

15546 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution III (2870699)

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

Risk Level: High

CVE: CVE-2013-3203

Update Details

Recommendation is updated

15547 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution IV (2870699)

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

Risk Level: High

CVE: CVE-2013-3204

Update Details

Recommendation is updated

15548 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution V (2870699)

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

Risk Level: High

CVE: CVE-2013-3205

Update Details

Recommendation is updated

15555 - (MS13-067) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)

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

Risk Level: High

CVE: CVE-2013-0081, CVE-2013-1315, CVE-2013-1330, CVE-2013-3179, CVE-2013-3180, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3857, CVE-2013-3858

Update Details

Recommendation is updated

15556 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VI (2870699)

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

Risk Level: High

CVE: CVE-2013-3206

Update Details

Recommendation is updated

15558 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VIII (2870699)

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

Risk Level: High

CVE: CVE-2013-3208

Update Details

Recommendation is updated

15562 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution IX (2870699)

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

Risk Level: High

CVE: CVE-2013-3209

Update Details

Recommendation is updated

15569 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution X (2870699)

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

Risk Level: High

CVE: CVE-2013-3845

Update Details

Recommendation is updated

15574 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VII (2870699)

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

Risk Level: High

CVE: CVE-2013-3207

Update Details

Recommendation is updated

15588 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution I (2858300)

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

Risk Level: High

CVE: CVE-2013-1315

Update Details

Recommendation is updated

15702 - (MS13-085) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080)

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

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3890

Update Details

Recommendation is updated

15703 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

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

Risk Level: High

CVE: CVE-2013-3889

Update Details

Recommendation is updated

15719 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

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

Risk Level: High

CVE: CVE-2013-3889

Update Details

Recommendation is updated

## 15720 - (MS13-080) Cumulative Security Update for Internet Explorer (2879017)

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

Risk Level: High

CVE: CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, CVE-2013-3893, CVE-2013-3897

### Update Details

Recommendation is updated

## 15721 - (MS13-084) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2885089)

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

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3895

### Update Details

Recommendation is updated

## 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

## 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

## 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

## 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

## 16045 - (MS13-100) Microsoft Sharepoint Page Content Privilege Escalation (2904244)

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

Risk Level: High

CVE: CVE-2013-5059

### Update Details

Recommendation is updated

## 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

## 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: High

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: High

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: High

CVE: CVE-2014-0260

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

---



## 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: High

CVE: CVE-2014-0267

### 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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

CVE: CVE-2014-0290

[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

16395 - (MS14-013) Vulnerability In Microsoft DirectShow Could Allow Remote Code Execution (2929961)

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

Risk Level: High

CVE: CVE-2014-0301

[Update Details](#)

Recommendation is updated

16396 - (MS14-013) Microsoft DirectShow Memory Corruption Remote Code Execution (2929961)

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

Risk Level: High

CVE: CVE-2014-0301

[Update Details](#)

Recommendation is updated

16405 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0324

[Update Details](#)

Recommendation is updated

16406 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0322

[Update Details](#)

Recommendation is updated

16407 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0321

[Update Details](#)

Recommendation is updated

16408 - (MS14-012) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0314

[Update Details](#)

Recommendation is updated

16409 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0313

[Update Details](#)

Recommendation is updated

16410 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0312

[Update Details](#)

Recommendation is updated

16411 - (MS14-012) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0311

[Update Details](#)

Recommendation is updated

16412 - (MS14-012) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0309

[Update Details](#)

Recommendation is updated

16413 - (MS14-012) Microsoft Internet Explorer Memory Corruption X Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0308

Update Details

Recommendation is updated

16414 - (MS14-012) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0307

Update Details

Recommendation is updated

16415 - (MS14-012) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0306

Update Details

Recommendation is updated

16416 - (MS14-012) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0305

Update Details

Recommendation is updated

16417 - (MS14-012) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0304

Update Details

Recommendation is updated



#### 16418 - (MS14-012) Microsoft Internet Explorer Memory Corruption V Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0303

##### Update Details

Recommendation is updated

#### 16419 - (MS14-012) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0302

##### Update Details

Recommendation is updated

#### 16420 - (MS14-012) Microsoft Internet Explorer Memory Corruption III Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0299

##### Update Details

Recommendation is updated

#### 16421 - (MS14-012) Microsoft Internet Explorer Memory Corruption II Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0298

##### Update Details

Recommendation is updated

#### 16422 - (MS14-012) Microsoft Internet Explorer Memory Corruption I Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0297

##### Update Details

Recommendation is updated

#### 16423 - (MS14-012) Cumulative Security Update for Internet Explorer (2925418)

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

Risk Level: High

CVE: CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, CVE-2014-0322, CVE-2014-0324

Update Details

Recommendation is updated

16460 - (MS12-052) Microsoft Internet Explorer Javascript Integer Overflow Remote Code Execution (2722913)

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

Risk Level: High

CVE: CVE-2012-2523

Update Details

Recommendation is updated

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

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: High

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: High

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: High

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: High

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: High

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: High

CVE: 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

#### 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: High

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: High

CVE: CVE-2014-1757

[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

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

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: High

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: High

CVE: CVE-2014-1815

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

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: High

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: High

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: High

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: High

CVE: CVE-2014-1803

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: High

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: High

CVE: CVE-2014-2753

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

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: High

CVE: CVE-2014-1795

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

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: High

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: High

CVE: CVE-2014-1797

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

16993 - Apple QuickTime mvhd Atom Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-4979

Update Details

Documentation 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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

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: High

CVE: CVE-2014-2799

### 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

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

17360 - (MS14-066) Microsoft Windows Schannel Remote Code Execution (2992611)

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

Risk Level: High

CVE: CVE-2014-6321

[Update Details](#)

Recommendation is updated

17361 - (MS14-068) Microsoft Windows Kerberos Checksum Privilege Escalation (3011780)

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

Risk Level: High

CVE: CVE-2014-6324

[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

## 17385 - (MS14-069) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6333 , CVE-2014-6334 , CVE-2014-6335

### Update Details

Recommendation is updated

## 17484 - (MS14-084) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)

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

Risk Level: High

CVE: CVE-2014-6363

### Update Details

Recommendation is updated

## 17488 - (MS14-081) Microsoft Word Index Remote Code Execution (3017301)

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

Risk Level: High

CVE: CVE-2014-6356

### Update Details

Recommendation is updated

## 17489 - (MS14-081) Microsoft Word Use-After-Free Remote Code Execution (3017301)

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

Risk Level: High

CVE: CVE-2014-6357

### Update Details

Recommendation is updated FASLScript is updated



17495 - (MS14-084) Microsoft VBScript Memory Corruption Remote Code Execution (3016711)

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

Risk Level: High

CVE: CVE-2014-6363

Update Details

Recommendation is updated

17498 - (MS14-080) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6327

Update Details

Recommendation is updated

17499 - (MS14-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6329

Update Details

Recommendation is updated

17500 - (MS14-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6330

Update Details

Recommendation is updated

17501 - (MS14-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6366

Update Details

Recommendation is updated

17502 - (MS14-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3008923)

---

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

Risk Level: High

CVE: CVE-2014-6369

[Update Details](#)

Recommendation is updated

#### 17503 - (MS14-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6373

[Update Details](#)

Recommendation is updated

#### 17504 - (MS14-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6374

[Update Details](#)

Recommendation is updated

#### 17505 - (MS14-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6375

[Update Details](#)

Recommendation is updated

#### 17506 - (MS14-080) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6376

[Update Details](#)

Recommendation is updated

#### 17507 - (MS14-080) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3008923)

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

Risk Level: High  
CVE: CVE-2014-8966

Update Details

Recommendation is updated

17508 - (MS14-080) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3008923)

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

Risk Level: High  
CVE: CVE-2014-6363

Update Details

Recommendation is updated

17512 - (MS14-080) Cumulative Security Update for Internet Explorer (3008923)

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

Risk Level: High  
CVE: CVE-2014-6327, CVE-2014-6328, CVE-2014-6329, CVE-2014-6330, CVE-2014-6363, CVE-2014-6365, CVE-2014-6366, CVE-2014-6368, CVE-2014-6369, CVE-2014-6373, CVE-2014-6374, CVE-2014-6375, CVE-2014-6376, CVE-2014-8966

Update Details

Recommendation is updated Risk is updated

4093 - (MS06-005) Microsoft Windows Media Player Code Execution

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

Risk Level: High  
CVE: CVE-2006-0006

Update Details

Recommendation is updated

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

#### 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

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

#### 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

#### 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

#### 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

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

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

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

6157 - (MS08-057) Microsoft Excel Calendar Object Validation Vulnerability (956416)

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

Risk Level: High

CVE: CVE-2008-3477

Update Details

Recommendation is updated

6158 - (MS08-057) Microsoft Excel File Format Parsing Vulnerability (956416)

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

Risk Level: High

CVE: CVE-2008-3471

Update Details

Recommendation is updated

6159 - (MS08-057) Microsoft Excel Format Parsing Vulnerability (956416)

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

Risk Level: High

CVE: CVE-2008-4019

Update Details

Recommendation is updated

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 Word RTF 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

6459 - (MS09-009) Microsoft Office Excel Memory Corruption Vulnerability II (968557)

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

Risk Level: High

CVE: CVE-2009-0238

Update Details

Recommendation is updated

6595 - (MS09-009) Microsoft Office Excel Memory Corruption Vulnerability (968557)

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

Risk Level: High

CVE: CVE-2009-0100

Update Details

Recommendation is updated

6607 - (MS09-014) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (963027)

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

Risk Level: High

CVE: CVE-2009-0552

Update Details

Recommendation is updated



## 6608 - (MS09-014) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability II (963027)

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

Risk Level: High

CVE: CVE-2009-0553

### Update Details

Recommendation is updated

## 6609 - (MS09-014) Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability III (963027)

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

Risk Level: High

CVE: CVE-2009-0554

### Update Details

Recommendation is updated

## 6754 - (MS09-021) Microsoft Office Excel Array Indexing Memory Corruption Vulnerability (969462)

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

Risk Level: High

CVE: CVE-2009-0558

### Update Details

Recommendation is updated

## 6755 - (MS09-021) Microsoft Office Excel Field Sensitization Memory Corruption Vulnerability (969462)

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

Risk Level: High

CVE: CVE-2009-0560

### Update Details

Recommendation is updated

## 6756 - (MS09-021) Microsoft Office Excel Object Record Corruption Vulnerability (969462)

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

Risk Level: High

CVE: CVE-2009-0557

### Update Details

Recommendation is updated

## 6757 - (MS09-021) Microsoft Office Excel Record Integer Overflow Vulnerability (969462)

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

Risk Level: High

CVE: CVE-2009-0561

Update Details

Recommendation is updated

6758 - (MS09-021) Microsoft Office Excel Record Pointer Corruption Vulnerability (969462)

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

Risk Level: High

CVE: CVE-2009-0549

Update Details

Recommendation is updated

6760 - (MS09-021) Microsoft Office Excel String Copy Stack-Based Overrun Vulnerability (969462)

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

Risk Level: High

CVE: CVE-2009-0559

Update Details

Recommendation is updated

6771 - (MS09-027) Microsoft Office Word Buffer Overflow Vulnerability (969514)

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

Risk Level: High

CVE: CVE-2009-0563

Update Details

Recommendation is updated

6772 - (MS09-027) Microsoft Office Word Buffer Overflow Vulnerability II (969514)

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

Risk Level: High

CVE: CVE-2009-0565

Update Details

Recommendation is updated

6903 - (MS09-060) ATL Null String Vulnerability (973965)

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

Risk Level: High

CVE: CVE-2009-2495

Update Details

Recommendation is updated

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

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

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

## 12211 - (MS11-045) Microsoft Excel Memory Corruption Remote Code Execution (2537146)

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

Risk Level: High

CVE: CVE-2011-1277

### Update Details

Recommendation is updated

## 12217 - (MS11-045) Microsoft Excel Out Of Bounds WriteAV Remote Code Execution (2537146)

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

Risk Level: High

CVE: CVE-2011-1279

### Update Details

Recommendation is updated

## 12257 - (MS11-045) Microsoft Excel WriteAV Remote Code Execution (2537146)

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

Risk Level: High

CVE: CVE-2011-1278

### Update Details

Recommendation is updated

## 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

## 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

## 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

## 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

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

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

17326 - MariaDB Multiple Vulnerabilities Prior To 5.5.40

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

Risk Level: High

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

Update Details

Recommendation is updated Risk is updated

1600 - (MS03-008) Windows Script Engine Code Execution

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

Risk Level: High

CVE: CVE-2003-0010

Update Details

Recommendation is updated

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

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

4729 - (MS06-071) Microsoft XML Core Services Remote Code Execution Vulnerability (928088)

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

Risk Level: High

CVE: CVE-2006-5745

Update Details

Recommendation is updated

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

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

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

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

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

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

### 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

### 17483 - (MS14-082) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3017349)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6364

[Update Details](#)

Recommendation is updated

### 142519 - SuSE SLES 10 SP4 firefox31-201411-8991 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

[Update Details](#)

FASLScript 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

### 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

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

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

9086 - (MS10-041) Microsoft Windows .NET Framework XML Signature HMAC Truncation Bypass Vulnerability (981343)

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

Risk Level: Medium  
CVE: CVE-2009-0217

[Update Details](#)

Recommendation is updated

16046 - (MS13-100) Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (2904244)

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

Risk Level: Medium  
CVE: CVE-2013-5059

[Update Details](#)

Recommendation is updated

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

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

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

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

9069 - (MS10-041) Vulnerabilities In The Microsoft .NET Framework Could Allow Tampering (981343)

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

Risk Level: Medium

CVE: CVE-2009-0217

Update Details

Recommendation is updated

9077 - (MS10-035) Microsoft Internet Explorer toStaticHTML Information Disclosure Vulnerability (982381)

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

Risk Level: Medium

CVE: CVE-2010-1257

Update Details

Recommendation is updated

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

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

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

#### 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

#### 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

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

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

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

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

15509 - MariaDB Multiple Denial of Service Vulnerabilities Prior To 5.5.32

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

Risk Level: Medium

CVE: CVE-2013-1861, CVE-2013-3783, CVE-2013-3793, CVE-2013-3802, CVE-2013-3804, CVE-2013-3809, CVE-2013-3812

Update Details

Recommendation is updated Risk is updated CVE 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

---

15590 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution II (2858300)

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

Risk Level: Medium

CVE: CVE-2013-3158

Update Details

Recommendation is updated

15592 - (MS13-073) Microsoft Office XML External Entities Resolution Information Disclosure (2858300)

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

Risk Level: Medium

CVE: CVE-2013-3159

Update Details

Recommendation is updated

15704 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution II (2885080)

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

Risk Level: Medium

CVE: CVE-2013-3890

Update Details

Recommendation is updated

15706 - (MS13-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3872

Update Details

Recommendation is updated

15707 - (MS13-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3873

Update Details

Recommendation is updated

15708 - (MS13-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3874

Update Details

Recommendation is updated

15709 - (MS13-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3875

Update Details

Recommendation is updated

15710 - (MS13-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3882

Update Details

Recommendation is updated

15712 - (MS13-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3885

Update Details

Recommendation is updated

15713 - (MS13-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3886

Update Details

Recommendation is updated

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

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

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

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

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

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

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

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

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

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

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

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

17401 - (MS14-075) Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6319, CVE-2014-6325, CVE-2014-6326, CVE-2014-6336

[Update Details](#)

Recommendation is updated

17402 - (MS14-075) Microsoft Exchange Server OWA URL Redirection Spoofing Information Disclosure (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6336

[Update Details](#)

Recommendation is updated

17403 - (MS14-075) Microsoft Exchange Server OWA Cross-Site Scripting II (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6326

Update Details

Recommendation is updated

17404 - (MS14-075) Microsoft Exchange Server OWA Cross-Site Scripting I (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6325

Update Details

Recommendation is updated

17405 - (MS14-075) Microsoft Exchange Server OWA Token Spoofing Information Disclosure (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6319

Update Details

Recommendation is updated

17481 - (MS14-085) Vulnerability in Microsoft Graphics Component Could Allow Information (3013126)

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

Risk Level: Medium

CVE: CVE-2014-6355

Update Details

Recommendation is updated

17490 - (MS14-083) Microsoft Excel Global Free Remote Code Execution (3017347)

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

Risk Level: Medium

CVE: CVE-2014-6360

Update Details

Recommendation is updated

17491 - (MS14-083) Microsoft Excel Invalid Pointer Remote Code Execution (3017347)

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

Risk Level: Medium

CVE: CVE-2014-6361

[Update Details](#)

Recommendation is updated

17492 - (MS14-085) Microsoft Graphics ASLR Bypass Information Disclosure (3013126)

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

Risk Level: Medium

CVE: CVE-2014-6355

[Update Details](#)

Recommendation is updated

17494 - (MS14-082) Microsoft Office Component Use-After-Free Remote Code Execution (3017349)

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

Risk Level: Medium

CVE: CVE-2014-6364

[Update Details](#)

Recommendation is updated

17497 - (MS14-080) Microsoft Internet Explorer ASLR Security Bypass (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6368

[Update Details](#)

Recommendation is updated

17509 - (MS14-080) Microsoft Internet Explorer XSS Filter I Security Bypass (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6328

[Update Details](#)

Recommendation is updated

17510 - (MS14-080) Microsoft Internet Explorer XSS Filter II Security Bypass (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6365

[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

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

12231 - (MS11-049) Microsoft XML Editor Could Allow Information Disclosure (2543893)

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

Risk Level: Medium

CVE: CVE-2011-1280

Update Details

Recommendation is updated

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

16503 - MariaDB Multiple Vulnerabilities Prior To 5.5.36

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

Risk Level: Medium

CVE: CVE-2014-0384, CVE-2014-2419, CVE-2014-2432, CVE-2014-2438, CVE-2014-4243

Update Details

Recommendation is updated Risk is updated CVE is updated

6967 - (MS09-036) Microsoft Remote Unauthenticated Denial of Service in ASP.NET Vulnerability (970957)

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

Risk Level: Low

CVE: CVE-2009-1536

Update Details

Recommendation is updated

6974 - (MS09-036) Microsoft Remote Unauthenticated Denial of Service in ASP.NET Vulnerability (970957)  
(Intrusive)

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

Risk Level: Low

CVE: CVE-2009-1536

Update Details

Recommendation is updated

7420 - (MS09-036) Vulnerability In ASP.NET In Microsoft Windows Could Allow Denial Of Service (970957)

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

Risk Level: Low

CVE: CVE-2009-1536

Update Details

Recommendation is updated

10345 - (MS10-071) Microsoft Internet Explorer Autocomplete Information Disclosure (2360131)

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

Risk Level: Low

CVE: CVE-2010-0808

Update Details

Recommendation is updated

12212 - (MS11-049) Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure  
(2543893)

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

Risk Level: Low

CVE: CVE-2011-1280

Update Details

Recommendation is updated

12447 - (MS11-057) Microsoft Internet Explorer Drag And Drop Information Disclosure (2559049)

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

Risk Level: Low

CVE: CVE-2011-2383

#### Update Details

Recommendation is updated

## DELETED CHECKS

### 43101 - HP-UX 11.X PHCO\_43389 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### 43114 - HP-UX 11.X PHSS\_43701 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: High

CVE: CVE-MAP-NOMATCH

## ADDITIONAL NOTES

- 43101 - was flagged as obsolete by the vendor.
- 43114 - was flagged as obsolete by the vendor.

## 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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2014 McAfee, Inc.  
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates