2015-NOV-26
FSL version 7.5.766

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

19311 - IBM WebSphere Application Server Apache Commons Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2015-7450

Description

A Java object deserialization vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a Java application server.

A Java object deserialization vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Apache Commons Collections. Successful exploitation could allow an attacker to execute arbitrary code.

91947 - Oracle Enterprise Linux ELSA-2015-2086 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
ELSA-2015-2086

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005550.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005548.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005551.html

OEL6
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7

i386

java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7

OEL5
x86_64
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.0.1.el5_11

i386
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.0.1.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.0.1.el5_11

OEL7
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el7_1

140978 - Red Hat Enterprise Linux RHSA-2015-2506 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4810, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4871, CVE-2015-4872, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4902, CVE-2015-4903, CVE-2015-5006

Description

The scan detected that the host is missing the following update:
RHSA-2015-2506

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2506.html

RHEL7S
ppc64
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el7

RHEL6S
i386

java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el6_7

x86_64
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el6_7

RHEL6WS
x86_64
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el6_7

i386
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el6_7

RHEL7D
x86_64
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el7

RHEL6D
x86_64
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el6_7

i386
java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el6_7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el6_7

RHEL7WS
x86_64

java-1.7.1-ibm-devel-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-src-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.3.20-1jpp.1.el7
java-1.7.1-ibm-1.7.1.3.20-1jpp.1.el7

140984 - Red Hat Enterprise Linux RHSA-2015-2509 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4810, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4871, CVE-2015-4872, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4902, CVE-2015-4903, CVE-2015-5006

Description

The scan detected that the host is missing the following update:
RHSA-2015-2509

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2509.html

RHEL7D
x86_64
java-1.8.0-ibm-demo-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-src-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-1.8.0.2.0-1jpp.1.el7

RHEL7S
ppc64
java-1.8.0-ibm-demo-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-src-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-1.8.0.2.0-1jpp.1.el7

RHEL7WS
x86_64
java-1.8.0-ibm-demo-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-src-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.2.0-1jpp.1.el7
java-1.8.0-ibm-1.8.0.2.0-1jpp.1.el7

140993 - Red Hat Enterprise Linux RHSA-2015-2507 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4810, CVE-2015-4835, CVE-2015-4840, CVE-

2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4871, CVE-2015-4872, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4902, CVE-2015-4903, CVE-2015-5006

Description

The scan detected that the host is missing the following update:
RHSA-2015-2507

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2507.html

RHEL5D
x86_64
java-1.7.0-ibm-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-devel-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-demo-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-plugin-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-jdbc-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-src-1.7.0.9.20-1jpp.1.el5

i386
java-1.7.0-ibm-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-devel-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-demo-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-plugin-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-jdbc-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-src-1.7.0.9.20-1jpp.1.el5

RHEL5S
i386
java-1.7.0-ibm-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-devel-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-demo-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-plugin-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-jdbc-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-src-1.7.0.9.20-1jpp.1.el5

x86_64
java-1.7.0-ibm-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-devel-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-demo-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-plugin-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-jdbc-1.7.0.9.20-1jpp.1.el5
java-1.7.0-ibm-src-1.7.0.9.20-1jpp.1.el5

141006 - Red Hat Enterprise Linux RHSA-2015-2508 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4902, CVE-2015-4903, CVE-2015-5006

Description

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

RHSA-2015-2508

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2508.html

RHEL5S
i386
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-accessibility-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el5

x86_64
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-accessibility-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el5

RHEL6D
x86_64
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el6_7

i386
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el6_7

RHEL6S
i386
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el6_7

x86_64
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el6_7

java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el6_7

RHEL6WS
x86_64
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el6_7

i386
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el6_7
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el6_7

RHEL5D
x86_64
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-accessibility-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el5

i386
java-1.6.0-ibm-devel-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-plugin-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-src-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-jdbc-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-javacomm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-accessibility-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-1.6.0.16.15-1jpp.1.el5
java-1.6.0-ibm-demo-1.6.0.16.15-1jpp.1.el5

141015 - Red Hat Enterprise Linux RHSA-2015-2086 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
RHSA-2015-2086

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2086.html

RHEL5S
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11

i386
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11

RHEL7S
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el7_1

RHEL6S
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7

i386
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7

RHEL6WS
x86_64
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7

i386
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7

java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7

RHEL5D
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11

i386
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11

RHEL7D
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el7_1

RHEL6D
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7

i386
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7

RHEL7WS
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el7_1

144061 - SuSE SLES 10 SP4 SUSE-SU-2015:2081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4473, CVE-2015-4474, CVE-2015-4475, CVE-2015-4478, CVE-2015-4479, CVE-2015-4484, CVE-2015-4485, CVE-

2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4491, CVE-2015-4492, CVE-2015-4497, CVE-2015-4498, CVE-2015-4500, CVE-2015-4501, CVE-2015-4506, CVE-2015-4509, CVE-2015-4511, CVE-2015-4513, CVE-2015-4517, CVE-2015-4519, CVE-2015-4520, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2081-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001691.html

SuSE SLES 10 SP4
i586
mozilla-nss-3.19.2.1-0.5.1
MozillaFirefox-translations-38.4.0esr-0.7.1
mozilla-nss-devel-3.19.2.1-0.5.1
MozillaFirefox-38.4.0esr-0.7.1
MozillaFirefox-branding-SLED-38-0.5.3
mozilla-nss-tools-3.19.2.1-0.5.1
mozilla-nspr-devel-4.10.10-0.5.1
mozilla-nspr-4.10.10-0.5.1

x86_64
mozilla-nss-3.19.2.1-0.5.1
mozilla-nss-devel-3.19.2.1-0.5.1
mozilla-nspr-32bit-4.10.10-0.5.1
mozilla-nss-tools-3.19.2.1-0.5.1
mozilla-nspr-devel-4.10.10-0.5.1
mozilla-nss-32bit-3.19.2.1-0.5.1
mozilla-nspr-4.10.10-0.5.1

160002 - CentOS 5, 6, 7 CESA-2015-2086 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
CESA-2015-2086

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021505.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021507.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021506.html

CentOS 6

x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7

i686
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7

CentOS 7
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el7_1

CentOS 5
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11

i386
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11

19304 - LibreOffice OpenOffice PrinterSetup ODF Document Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-5212

Description

A vulnerability in some versions of LibreOffice and Apache OpenOffice could lead to remote code execution.

Observation

A vulnerability in some versions of LibreOffice and Apache OpenOffice could lead to remote code execution.

The flaw lies in the handling of a crafted ODF document. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

19317 - SolarWinds DameWare URI Handler Stack Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-8220

Description

A vulnerability in some versions of SolarWinds DameWare could lead to remote code execution.

Observation

A vulnerability in some versions of SolarWinds DameWare could lead to remote code execution.

The flaw exists within DWRCC.exe. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

19325 - Oracle WebLogic Server WLS Security Apache Commons Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-4852

Description

A vulnerability in some versions of Oracle WebLogic Server could lead to remote code execution.

Observation

A vulnerability in some versions of Oracle WebLogic Server could lead to remote code execution.

The flaw lies in the Apache Commons Collections library. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

190017 - Fedora Linux 21 FEDORA-2015-0f405832d3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7805

Description

The scan detected that the host is missing the following update:
FEDORA-2015-0f405832d3

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172607.html

Fedora Core 21

libsndfile-1.0.25-16.fc21

190024 - Fedora Linux 22 FEDORA-2015-56be43eae6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7805

Description

The scan detected that the host is missing the following update:
FEDORA-2015-56be43eae6

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172593.html

Fedora Core 22

libsndfile-1.0.25-17.fc22

91959 - Oracle Enterprise Linux ELSA-2015-2088 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5352, CVE-2015-5600, CVE-2015-6563, CVE-2015-6564

Description

The scan detected that the host is missing the following update:
ELSA-2015-2088

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005560.html

OEL7
x86_64
openssh-server-sysvinit-6.6.1p1-22.el7
openssh-keycat-6.6.1p1-22.el7
openssh-askpass-6.6.1p1-22.el7
openssh-6.6.1p1-22.el7
openssh-server-6.6.1p1-22.el7
pam_ssh_agent_auth-0.9.3-9.22.el7
openssh-clients-6.6.1p1-22.el7
openssh-ldap-6.6.1p1-22.el7

140992 - Red Hat Enterprise Linux RHSA-2015-2088 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5600, CVE-2015-6563, CVE-2015-6564

Description

The scan detected that the host is missing the following update:
RHSA-2015-2088

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2088.html

RHEL7D
x86_64
openssh-server-sysvinit-6.6.1p1-22.el7
openssh-keycat-6.6.1p1-22.el7
openssh-askpass-6.6.1p1-22.el7
openssh-debuginfo-6.6.1p1-22.el7
openssh-server-6.6.1p1-22.el7
pam_ssh_agent_auth-0.9.3-9.22.el7
openssh-clients-6.6.1p1-22.el7
openssh-6.6.1p1-22.el7
openssh-ldap-6.6.1p1-22.el7

RHEL7WS
x86_64
openssh-server-sysvinit-6.6.1p1-22.el7
openssh-keycat-6.6.1p1-22.el7
openssh-askpass-6.6.1p1-22.el7
openssh-debuginfo-6.6.1p1-22.el7
openssh-server-6.6.1p1-22.el7
pam_ssh_agent_auth-0.9.3-9.22.el7
openssh-clients-6.6.1p1-22.el7
openssh-6.6.1p1-22.el7
openssh-ldap-6.6.1p1-22.el7

144065 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2055-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2698

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2055-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00116.html

SuSE Linux 13.1
x86_64
krb5-mini-devel-1.11.3-3.24.1
krb5-1.11.3-3.24.1
krb5-debuginfo-32bit-1.11.3-3.24.1
krb5-plugin-kdb-ldap-1.11.3-3.24.1
krb5-doc-1.11.3-3.24.1
krb5-plugin-preauth-pkinit-debuginfo-1.11.3-3.24.1
krb5-mini-1.11.3-3.24.1
krb5-debugsource-1.11.3-3.24.1
krb5-server-debuginfo-1.11.3-3.24.1
krb5-client-1.11.3-3.24.1
krb5-debuginfo-1.11.3-3.24.1
krb5-32bit-1.11.3-3.24.1
krb5-plugin-preauth-pkinit-1.11.3-3.24.1
krb5-client-debuginfo-1.11.3-3.24.1

krb5-server-1.11.3-3.24.1
krb5-mini-debuginfo-1.11.3-3.24.1
krb5-devel-1.11.3-3.24.1
krb5-devel-32bit-1.11.3-3.24.1
krb5-mini-debugsource-1.11.3-3.24.1
krb5-plugin-kdb-ldap-debuginfo-1.11.3-3.24.1

i586
krb5-mini-devel-1.11.3-3.24.1
krb5-1.11.3-3.24.1
krb5-plugin-kdb-ldap-1.11.3-3.24.1
krb5-doc-1.11.3-3.24.1
krb5-plugin-preauth-pkinit-debuginfo-1.11.3-3.24.1
krb5-mini-1.11.3-3.24.1
krb5-debugsource-1.11.3-3.24.1
krb5-server-debuginfo-1.11.3-3.24.1
krb5-client-1.11.3-3.24.1
krb5-debuginfo-1.11.3-3.24.1
krb5-plugin-preauth-pkinit-1.11.3-3.24.1
krb5-client-debuginfo-1.11.3-3.24.1
krb5-server-1.11.3-3.24.1
krb5-mini-debuginfo-1.11.3-3.24.1
krb5-devel-1.11.3-3.24.1
krb5-mini-debugsource-1.11.3-3.24.1
krb5-plugin-kdb-ldap-debuginfo-1.11.3-3.24.1

SuSE Linux 13.2
x86_64
krb5-plugin-preauth-otp-1.12.2-18.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.2-18.1
krb5-plugin-preauth-otp-debuginfo-1.12.2-18.1
krb5-server-debuginfo-1.12.2-18.1
krb5-server-1.12.2-18.1
krb5-debuginfo-1.12.2-18.1
krb5-plugin-kdb-ldap-debuginfo-1.12.2-18.1
krb5-debugsource-1.12.2-18.1
krb5-plugin-kdb-ldap-1.12.2-18.1
krb5-client-debuginfo-1.12.2-18.1
krb5-plugin-preauth-pkinit-1.12.2-18.1
krb5-devel-1.12.2-18.1
krb5-mini-debuginfo-1.12.2-18.1
krb5-mini-debugsource-1.12.2-18.1
krb5-devel-32bit-1.12.2-18.1
krb5-mini-devel-1.12.2-18.1
krb5-1.12.2-18.1
krb5-doc-1.12.2-18.1
krb5-debuginfo-32bit-1.12.2-18.1
krb5-32bit-1.12.2-18.1
krb5-mini-1.12.2-18.1
krb5-client-1.12.2-18.1

i586
krb5-plugin-preauth-otp-1.12.2-18.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.2-18.1
krb5-plugin-preauth-otp-debuginfo-1.12.2-18.1
krb5-server-debuginfo-1.12.2-18.1
krb5-server-1.12.2-18.1
krb5-debuginfo-1.12.2-18.1
krb5-plugin-kdb-ldap-debuginfo-1.12.2-18.1
krb5-debugsource-1.12.2-18.1

krb5-plugin-kdb-ldap-1.12.2-18.1
krb5-client-debuginfo-1.12.2-18.1
krb5-plugin-preauth-pkinit-1.12.2-18.1
krb5-devel-1.12.2-18.1
krb5-mini-debuginfo-1.12.2-18.1
krb5-mini-debugsource-1.12.2-18.1
krb5-mini-devel-1.12.2-18.1
krb5-1.12.2-18.1
krb5-doc-1.12.2-18.1
krb5-mini-1.12.2-18.1
krb5-client-1.12.2-18.1

190013 - Fedora Linux 21 FEDORA-2015-200d2dfd9f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2695, CVE-2015-2696, CVE-2015-2697, CVE-2015-2698

Description

The scan detected that the host is missing the following update:
FEDORA-2015-200d2dfd9f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172665.html

Fedora Core 21

krb5-1.12.2-19.fc21

190035 - Fedora Linux 22 FEDORA-2015-1b9c33d713 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2695, CVE-2015-2696, CVE-2015-2697, CVE-2015-2698

Description

The scan detected that the host is missing the following update:
FEDORA-2015-1b9c33d713

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172121.html

Fedora Core 22

krb5-1.13.2-10.fc22

19297 - Apache OpenOffice Multiple Vulnerabilities Prior To 4.1.2

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1774, CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

Multiple vulnerabilities are present in some versions of Apache OpenOffice.

Observation

Apache OpenOffice is an open source office software suite.

Multiple vulnerabilities are present in some versions of Apache OpenOffice. The flaws lie in several components. Successful exploitation requires the use of a maliciously crafted DOC, ODF or HWP file, and could allow an attacker to cause a denial of service, remote code execution or information disclosure.

19313 - TECO AP-PCLINK TPC File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of TECO AP-PCLINK could lead to remote code execution.

Observation

A vulnerability in some versions of TECO AP-PCLINK could lead to remote code execution.

The flaw lies in the handling of a TPC file. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

19316 - TECO TP3-PCLINK TPC File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of TECO TP3-PCLINK could lead to remote code execution.

Observation

A vulnerability in some versions of TECO TP3-PCLINK could lead to remote code execution.

The flaw lies in the handling of a TPC file. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

91940 - Oracle Enterprise Linux ELSA-2015-2393 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714, CVE-2015-0562, CVE-2015-0563, CVE-2015-0564, CVE-2015-2188, CVE-2015-2189, CVE-2015-2191, CVE-2015-3182, CVE-2015-3810, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813, CVE-2015-6243, CVE-2015-6244, CVE-2015-6245, CVE-2015-6246, CVE-2015-6248

Description

The scan detected that the host is missing the following update:
ELSA-2015-2393

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005575.html

OEL7
x86_64
wireshark-devel-1.10.14-7.0.1.el7
wireshark-gnome-1.10.14-7.0.1.el7
wireshark-1.10.14-7.0.1.el7

91944 - Oracle Enterprise Linux ELSA-2015-2079 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8484, CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8503, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

Description

The scan detected that the host is missing the following update:
ELSA-2015-2079

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005576.html

OEL7
x86_64
binutils-devel-2.23.52.0.1-55.el7
binutils-2.23.52.0.1-55.el7

91949 - Oracle Enterprise Linux ELSA-2015-2360 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4337, CVE-2014-4338, CVE-2015-3258, CVE-2015-3279

Description

The scan detected that the host is missing the following update:
ELSA-2015-2360

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005570.html

OEL7
x86_64
cups-filters-libs-1.0.35-21.el7
cups-filters-1.0.35-21.el7
cups-filters-devel-1.0.35-21.el7

91952 - Oracle Enterprise Linux ELSA-2015-2155 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0207, CVE-2014-0237, CVE-2014-0238, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3538, CVE-2014-3587, CVE-2014-3710, CVE-2014-8116, CVE-2014-8117, CVE-2014-9652, CVE-2014-9653

Description

The scan detected that the host is missing the following update:
ELSA-2015-2155

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005562.html

OEL7
x86_64
file-devel-5.11-31.el7
file-libs-5.11-31.el7
file-static-5.11-31.el7
python-magic-5.11-31.el7
file-5.11-31.el7

130317 - Debian Linux 7.0, 8.0 DSA-3399-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
DSA-3399-1

Observation

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

http://www.debian.org/security/2015/dsa-3399

Debian 8.0
all
libpng3_1.2.50-2+deb8u1
libpng12-0_1.2.50-2+deb8u1
libpng12-0-udeb_1.2.50-2+deb8u1
libpng12-dev_1.2.50-2+deb8u1

Debian 7.0
all

libpng12-dev_1.2.49-1+deb7u1
libpng12-0-udeb_1.2.49-1+deb7u1
libpng3_1.2.49-1+deb7u1
libpng12-0_1.2.49-1+deb7u1

130318 - Debian Linux 8.0 DSA-3400-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1335

Description

The scan detected that the host is missing the following update:
DSA-3400-1

Observation

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

http://www.debian.org/security/2015/dsa-3400

Debian 8.0
all
lxc_1:1.0.6-6+deb8u2

140977 - Red Hat Enterprise Linux RHSA-2015-2172 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5277

Description

The scan detected that the host is missing the following update:
RHSA-2015-2172

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2172.html

RHEL7D
x86_64
glibc-devel-2.17-106.el7_2.1
glibc-static-2.17-106.el7_2.1
glibc-utils-2.17-106.el7_2.1
glibc-2.17-106.el7_2.1
glibc-debuginfo-2.17-106.el7_2.1
glibc-debuginfo-common-2.17-106.el7_2.1
glibc-headers-2.17-106.el7_2.1
nscd-2.17-106.el7_2.1
glibc-common-2.17-106.el7_2.1

RHEL7WS
x86_64
glibc-devel-2.17-106.el7_2.1

glibc-static-2.17-106.el7_2.1
glibc-utils-2.17-106.el7_2.1
glibc-2.17-106.el7_2.1
glibc-debuginfo-2.17-106.el7_2.1
glibc-debuginfo-common-2.17-106.el7_2.1
glibc-headers-2.17-106.el7_2.1
nscd-2.17-106.el7_2.1
glibc-common-2.17-106.el7_2.1

140981 - Red Hat Enterprise Linux RHSA-2015-2199 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7423, CVE-2015-1472, CVE-2015-1473, CVE-2015-1781

Description

The scan detected that the host is missing the following update:
RHSA-2015-2199

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2199.html

RHEL7D
x86_64
glibc-2.17-105.el7
glibc-common-2.17-105.el7
glibc-headers-2.17-105.el7
glibc-static-2.17-105.el7
glibc-devel-2.17-105.el7
nscd-2.17-105.el7
glibc-debuginfo-2.17-105.el7
glibc-utils-2.17-105.el7
glibc-debuginfo-common-2.17-105.el7

RHEL7WS
x86_64
glibc-2.17-105.el7
glibc-common-2.17-105.el7
glibc-headers-2.17-105.el7
glibc-static-2.17-105.el7
glibc-devel-2.17-105.el7
nscd-2.17-105.el7
glibc-debuginfo-2.17-105.el7
glibc-utils-2.17-105.el7
glibc-debuginfo-common-2.17-105.el7

140982 - Red Hat Enterprise Linux RHSA-2015-2360 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3258, CVE-2015-3279

Description

The scan detected that the host is missing the following update:
RHSA-2015-2360

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2360.html

RHEL7D
x86_64
cups-filters-libs-1.0.35-21.el7
cups-filters-1.0.35-21.el7
cups-filters-devel-1.0.35-21.el7
cups-filters-debuginfo-1.0.35-21.el7

RHEL7WS
x86_64
cups-filters-libs-1.0.35-21.el7
cups-filters-1.0.35-21.el7
cups-filters-devel-1.0.35-21.el7
cups-filters-debuginfo-1.0.35-21.el7

140983 - Red Hat Enterprise Linux RHSA-2015-2393 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714, CVE-2015-0562, CVE-2015-0563, CVE-2015-0564, CVE-2015-2188, CVE-2015-2189, CVE-2015-2191, CVE-2015-3182, CVE-2015-3810, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813, CVE-2015-6243, CVE-2015-6244, CVE-2015-6245, CVE-2015-6246, CVE-2015-6248

Description

The scan detected that the host is missing the following update:
RHSA-2015-2393

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2393.html

RHEL7D
x86_64
wireshark-gnome-1.10.14-7.el7
wireshark-1.10.14-7.el7
wireshark-devel-1.10.14-7.el7
wireshark-debuginfo-1.10.14-7.el7

RHEL7WS
x86_64
wireshark-gnome-1.10.14-7.el7
wireshark-1.10.14-7.el7
wireshark-devel-1.10.14-7.el7
wireshark-debuginfo-1.10.14-7.el7

140985 - Red Hat Enterprise Linux RHSA-2015-2079 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8484, CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8503, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

Description

The scan detected that the host is missing the following update:
RHSA-2015-2079

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2079.html

RHEL7D
x86_64
binutils-devel-2.23.52.0.1-55.el7
binutils-2.23.52.0.1-55.el7
binutils-debuginfo-2.23.52.0.1-55.el7

RHEL7WS
x86_64
binutils-devel-2.23.52.0.1-55.el7
binutils-2.23.52.0.1-55.el7
binutils-debuginfo-2.23.52.0.1-55.el7

140991 - Red Hat Enterprise Linux RHSA-2015-2068 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7181, CVE-2015-7182, CVE-2015-7183

Description

The scan detected that the host is missing the following update:
RHSA-2015-2068

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2068.html

RHEL6_6S
i386
nss-util-3.19.1-2.el6_6
nspr-4.10.8-2.el6_6
nspr-devel-4.10.8-2.el6_6
nss-devel-3.19.1-4.el6_6
nss-debuginfo-3.19.1-4.el6_6
nss-util-devel-3.19.1-2.el6_6
nss-sysinit-3.19.1-4.el6_6
nss-util-debuginfo-3.19.1-2.el6_6
nspr-debuginfo-4.10.8-2.el6_6
nss-3.19.1-4.el6_6
nss-tools-3.19.1-4.el6_6

x86_64
nss-util-3.19.1-2.el6_6
nspr-4.10.8-2.el6_6
nspr-devel-4.10.8-2.el6_6
nss-devel-3.19.1-4.el6_6
nss-debuginfo-3.19.1-4.el6_6
nss-util-devel-3.19.1-2.el6_6
nss-sysinit-3.19.1-4.el6_6
nss-util-debuginfo-3.19.1-2.el6_6
nspr-debuginfo-4.10.8-2.el6_6
nss-3.19.1-4.el6_6
nss-tools-3.19.1-4.el6_6

RHEL6_5S
i386
nss-util-devel-3.16.1-3.el6_5
nss-debuginfo-3.16.1-9.el6_5
nspr-devel-4.10.6-2.el6_5
nss-tools-3.16.1-9.el6_5
nss-3.16.1-9.el6_5
nss-pkcs11-devel-3.16.1-9.el6_5
nss-util-debuginfo-3.16.1-3.el6_5
nspr-debuginfo-4.10.6-2.el6_5
nss-util-3.16.1-3.el6_5
nss-sysinit-3.16.1-9.el6_5
nspr-4.10.6-2.el6_5
nss-devel-3.16.1-9.el6_5

x86_64
nss-util-devel-3.16.1-3.el6_5
nss-debuginfo-3.16.1-9.el6_5
nspr-devel-4.10.6-2.el6_5
nss-tools-3.16.1-9.el6_5
nss-3.16.1-9.el6_5
nss-pkcs11-devel-3.16.1-9.el6_5
nss-util-debuginfo-3.16.1-3.el6_5
nspr-debuginfo-4.10.6-2.el6_5
nss-util-3.16.1-3.el6_5
nss-sysinit-3.16.1-9.el6_5
nspr-4.10.6-2.el6_5
nss-devel-3.16.1-9.el6_5

RHEL6_2S
x86_64
nss-util-debuginfo-3.13.1-9.el6_2
nss-devel-3.13.1-12.el6_2
nspr-4.8.9-6.el6_2
nspr-debuginfo-4.8.9-6.el6_2
nss-3.13.1-12.el6_2
nss-debuginfo-3.13.1-12.el6_2
nss-sysinit-3.13.1-12.el6_2
nss-util-devel-3.13.1-9.el6_2
nss-util-3.13.1-9.el6_2
nss-pkcs11-devel-3.13.1-12.el6_2
nss-tools-3.13.1-12.el6_2
nspr-devel-4.8.9-6.el6_2

141004 - Red Hat Enterprise Linux RHSA-2015-2233 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8240, CVE-2014-8241

Description

The scan detected that the host is missing the following update:
RHSA-2015-2233

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2233.html

RHEL7D
x86_64
tigervnc-1.3.1-3.el7
tigervnc-server-module-1.3.1-3.el7
tigervnc-server-minimal-1.3.1-3.el7
tigervnc-debuginfo-1.3.1-3.el7
tigervnc-server-1.3.1-3.el7

noarch
tigervnc-license-1.3.1-3.el7
tigervnc-icons-1.3.1-3.el7
tigervnc-server-applet-1.3.1-3.el7

RHEL7WS
x86_64
tigervnc-1.3.1-3.el7
tigervnc-server-module-1.3.1-3.el7
tigervnc-server-minimal-1.3.1-3.el7
tigervnc-debuginfo-1.3.1-3.el7
tigervnc-server-1.3.1-3.el7

noarch
tigervnc-license-1.3.1-3.el7
tigervnc-icons-1.3.1-3.el7
tigervnc-server-applet-1.3.1-3.el7

141013 - Red Hat Enterprise Linux RHSA-2015-2155 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1571, CVE-2014-0207, CVE-2014-0237, CVE-2014-0238, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3538, CVE-2014-3587, CVE-2014-3710, CVE-2014-8116, CVE-2014-8117, CVE-2014-9652, CVE-2014-9653

Description

The scan detected that the host is missing the following update:
RHSA-2015-2155

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2155.html

RHEL7D
x86_64
file-devel-5.11-31.el7
file-libs-5.11-31.el7
file-static-5.11-31.el7
file-debuginfo-5.11-31.el7
file-5.11-31.el7

noarch
python-magic-5.11-31.el7

RHEL7WS
x86_64
file-devel-5.11-31.el7
file-libs-5.11-31.el7
file-static-5.11-31.el7
file-debuginfo-5.11-31.el7
file-5.11-31.el7

noarch
python-magic-5.11-31.el7

144053 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2065-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0794

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2065-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001690.html

SuSE SLED 12
x86_64
dracut-037-51.17.3
dracut-debugsource-037-51.17.3
dracut-debuginfo-037-51.17.3

SuSE SLES 12
x86_64
dracut-037-51.17.3
dracut-debugsource-037-51.17.3
dracut-debuginfo-037-51.17.3
dracut-fips-037-51.17.3

144057 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2013-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2013-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001681.html

SuSE SLED 12
x86_64
libpng16-16-debuginfo-32bit-1.6.8-8.1
libpng16-16-32bit-1.6.8-8.1
libpng16-16-1.6.8-8.1
libpng16-16-debuginfo-1.6.8-8.1
libpng16-debugsource-1.6.8-8.1

SuSE SLES 12
x86_64
libpng16-16-debuginfo-32bit-1.6.8-8.1
libpng16-debugsource-1.6.8-8.1
libpng16-16-1.6.8-8.1
libpng16-16-debuginfo-1.6.8-8.1
libpng16-16-32bit-1.6.8-8.1

144058 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2056-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2056-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001687.html

SuSE SLED 12
x86_64
libksba8-debuginfo-1.3.0-12.1
libksba-debugsource-1.3.0-12.1
libksba8-1.3.0-12.1

SuSE SLES 12
x86_64
libksba8-debuginfo-1.3.0-12.1
libksba-debugsource-1.3.0-12.1
libksba8-1.3.0-12.1

144059 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2023-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5309

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2023-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00099.html

SuSE Linux 13.1
x86_64
putty-debuginfo-0.66-2.7.1
putty-0.66-2.7.1
putty-debugsource-0.66-2.7.1

i586
putty-debuginfo-0.66-2.7.1
putty-0.66-2.7.1
putty-debugsource-0.66-2.7.1

SuSE Linux 13.2
x86_64
putty-0.66-4.7.1
putty-debuginfo-0.66-4.7.1
putty-debugsource-0.66-4.7.1

i586
putty-0.66-4.7.1
putty-debuginfo-0.66-4.7.1
putty-debugsource-0.66-4.7.1

144060 - SuSE Linux 13.2 openSUSE-SU-2015:2022-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0794

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2022-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00098.html

SuSE Linux 13.2
x86_64
dracut-debugsource-037-17.30.1
dracut-037-17.30.1
dracut-debuginfo-037-17.30.1

dracut-fips-037-17.30.1

i586
dracut-debugsource-037-17.30.1
dracut-037-17.30.1
dracut-debuginfo-037-17.30.1
dracut-fips-037-17.30.1

144062 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2069-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1302

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2069-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00121.html

SuSE Linux 13.1
x86_64
chromium-desktop-kde-46.0.2490.86-112.1
chromium-debuginfo-46.0.2490.86-112.1
chromium-ffmpegsumo-46.0.2490.86-112.1
chromium-ffmpegsumo-debuginfo-46.0.2490.86-112.1
chromium-debugsource-46.0.2490.86-112.1
chromium-46.0.2490.86-112.1
chromium-desktop-gnome-46.0.2490.86-112.1
chromedriver-debuginfo-46.0.2490.86-112.1
chromedriver-46.0.2490.86-112.1

i586
chromium-desktop-kde-46.0.2490.86-112.1
chromium-debuginfo-46.0.2490.86-112.1
chromium-ffmpegsumo-46.0.2490.86-112.1
chromium-ffmpegsumo-debuginfo-46.0.2490.86-112.1
chromium-debugsource-46.0.2490.86-112.1
chromium-46.0.2490.86-112.1
chromium-desktop-gnome-46.0.2490.86-112.1
chromedriver-debuginfo-46.0.2490.86-112.1
chromedriver-46.0.2490.86-112.1

SuSE Linux 13.2
x86_64
chromium-debuginfo-46.0.2490.86-57.1
chromium-46.0.2490.86-57.1
chromium-ffmpegsumo-46.0.2490.86-57.1
chromium-debugsource-46.0.2490.86-57.1
chromium-desktop-kde-46.0.2490.86-57.1
chromium-ffmpegsumo-debuginfo-46.0.2490.86-57.1
chromedriver-debuginfo-46.0.2490.86-57.1
chromedriver-46.0.2490.86-57.1
chromium-desktop-gnome-46.0.2490.86-57.1

i586
chromium-debuginfo-46.0.2490.86-57.1
chromium-46.0.2490.86-57.1
chromium-ffmpegsumo-46.0.2490.86-57.1
chromium-debugsource-46.0.2490.86-57.1
chromium-desktop-kde-46.0.2490.86-57.1
chromium-ffmpegsumo-debuginfo-46.0.2490.86-57.1
chromedriver-debuginfo-46.0.2490.86-57.1
chromedriver-46.0.2490.86-57.1
chromium-desktop-gnome-46.0.2490.86-57.1

144063 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2024-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2024-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001683.html

SuSE SLED 12
x86_64
libpng12-0-1.2.50-10.1
libpng12-0-debuginfo-32bit-1.2.50-10.1
libpng12-0-32bit-1.2.50-10.1
libpng12-0-debuginfo-1.2.50-10.1
libpng12-debugsource-1.2.50-10.1

SuSE SLES 12
x86_64
libpng12-0-1.2.50-10.1
libpng12-0-debuginfo-32bit-1.2.50-10.1
libpng12-0-32bit-1.2.50-10.1
libpng12-0-debuginfo-1.2.50-10.1
libpng12-debugsource-1.2.50-10.1

144064 - SuSE SLES 12 SUSE-SU-2015:2025-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2025-1

Observation

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

For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001684.html

SuSE SLES 12
x86_64
git-core-debuginfo-1.8.5.6-14.3
git-debugsource-1.8.5.6-14.3
git-core-1.8.5.6-14.3

144066 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2057-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2057-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00117.html

SuSE Linux 13.1
x86_64
libksba-debugsource-1.3.0-5.7.1
libksba8-debuginfo-1.3.0-5.7.1
libksba-devel-1.3.0-5.7.1
libksba8-1.3.0-5.7.1

i586
libksba-debugsource-1.3.0-5.7.1
libksba8-debuginfo-1.3.0-5.7.1
libksba-devel-1.3.0-5.7.1
libksba8-1.3.0-5.7.1

SuSE Linux 13.2
x86_64
libksba-devel-1.3.1-7.1
libksba8-1.3.1-7.1
libksba-debugsource-1.3.1-7.1
libksba8-debuginfo-1.3.1-7.1

i586
libksba-devel-1.3.1-7.1
libksba8-1.3.1-7.1
libksba-debugsource-1.3.1-7.1
libksba8-debuginfo-1.3.1-7.1

144067 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2088-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2088-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001696.html

SuSE SLED 12
x86_64
libvncserver0-0.9.9-15.1
LibVNCServer-debugsource-0.9.9-15.1
libvncclient0-0.9.9-15.1
libvncclient0-debuginfo-0.9.9-15.1
libvncserver0-debuginfo-0.9.9-15.1

SuSE SLES 12
x86_64
libvncserver0-0.9.9-15.1
LibVNCServer-debugsource-0.9.9-15.1
libvncclient0-0.9.9-15.1
libvncclient0-debuginfo-0.9.9-15.1
libvncserver0-debuginfo-0.9.9-15.1

170588 - Amazon Linux AMI ALAS-2015-611 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126

Description

The scan detected that the host is missing the following update:
ALAS-2015-611

Observation

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

https://alas.aws.amazon.com/ALAS-2015-611.html

Amazon Linux AMI
x86_64
libpng-debuginfo-1.2.49-1.13.amzn1
libpng-1.2.49-1.13.amzn1
libpng-static-1.2.49-1.13.amzn1
libpng-devel-1.2.49-1.13.amzn1

i686
libpng-1.2.49-1.13.amzn1
libpng-debuginfo-1.2.49-1.13.amzn1
libpng-static-1.2.49-1.13.amzn1
libpng-devel-1.2.49-1.13.amzn1

170589 - Amazon Linux AMI ALAS-2015-612 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6816

Description

The scan detected that the host is missing the following update:
ALAS-2015-612

Observation

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

https://alas.aws.amazon.com/ALAS-2015-612.html

Amazon Linux AMI
x86_64
ganglia-gmond-3.7.2-2.19.amzn1
ganglia-web-3.7.1-2.19.amzn1
ganglia-devel-3.7.2-2.19.amzn1
ganglia-gmond-python-3.7.2-2.19.amzn1
ganglia-3.7.2-2.19.amzn1
ganglia-gmetad-3.7.2-2.19.amzn1
ganglia-debuginfo-3.7.2-2.19.amzn1

i686
ganglia-gmond-3.7.2-2.19.amzn1
ganglia-web-3.7.1-2.19.amzn1
ganglia-devel-3.7.2-2.19.amzn1
ganglia-3.7.2-2.19.amzn1
ganglia-gmetad-3.7.2-2.19.amzn1
ganglia-gmond-python-3.7.2-2.19.amzn1
ganglia-debuginfo-3.7.2-2.19.amzn1

181683 - FreeBSD mozilla Multiple Vulnerabilities (9d04936c-75f1-4a2c-9ade-4c1708be5df9)

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-4514, CVE-2015-4515, CVE-2015-4518, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7185, CVE-2015-7186, CVE-2015-7187, CVE-2015-7188, CVE-2015-7189, CVE-2015-7190, CVE-2015-7191, CVE-2015-7192, CVE-2015-7193, CVE-2015-7194, CVE-2015-7195, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (9d04936c-75f1-4a2c-9ade-4c1708be5df9)

Observation

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

http://www.vuxml.org/freebsd/9d04936c-75f1-4a2c-9ade-4c1708be5df9.html

Affected packages:
nspr < 4.10.10
3.20 <= nss < 3.20.1

3.19.3 <= nss < 3.19.4
nss < 3.19.2.1
firefox < 42.0,1
linux-firefox < 42.0,1
seamonkey < 2.39
linux-seamonkey < 2.39
firefox-esr < 38.4.0,1
libxul < 38.4.0
thunderbird < 38.4.0
linux-thunderbird < 38.4.0

181684 - FreeBSD gdm Lock Screen Bypass When Holding Escape Key (68847b20-8ddc-11e5-b69c-c86000169601)

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

Risk Level: High

CVE: CVE-2015-7496

Description

The scan detected that the host is missing the following update:
gdm -- lock screen bypass when holding escape key (68847b20-8ddc-11e5-b69c-c86000169601)

Observation

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

http://www.vuxml.org/freebsd/68847b20-8ddc-11e5-b69c-c86000169601.html

Affected packages:
gdm < 3.16.2_1

185061 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2815-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3425, CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
USN-2815-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003197.html

Ubuntu 12.04

libpng12-0_1.2.46-3ubuntu4.1

Ubuntu 15.04

libpng12-0_1.2.51-0ubuntu3.15.04.1

Ubuntu 15.10

libpng12-0_1.2.51-0ubuntu3.15.10.1

Ubuntu 14.04

libpng12-0_1.2.50-1ubuntu2.14.04.1

190010 - Fedora Linux 23 FEDORA-2015-1d87313b7c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
FEDORA-2015-1d87313b7c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172620.html

Fedora Core 23

libpng10-1.0.64-1.fc23

190015 - Fedora Linux 21 FEDORA-2015-501493d853 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
FEDORA-2015-501493d853

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172663.html

Fedora Core 21

libpng10-1.0.64-1.fc21

190016 - Fedora Linux 23 FEDORA-2015-5e52306c9c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126

Description

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

FEDORA-2015-5e52306c9c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172324.html

Fedora Core 23

libpng-1.6.17-4.fc23

190030 - Fedora Linux 23 FEDORA-2015-1dd5bc998f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5143, CVE-2015-5144, CVE-2015-5963, CVE-2015-5964

Description

The scan detected that the host is missing the following update:
FEDORA-2015-1dd5bc998f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172084.html

Fedora Core 23

python-django-1.8.6-1.fc23

190036 - Fedora Linux 23 FEDORA-2015-271025c598 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7496

Description

The scan detected that the host is missing the following update:
FEDORA-2015-271025c598

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172328.html

Fedora Core 23

gdm-3.18.2-1.fc23

190044 - Fedora Linux 22 FEDORA-2015-ec2ddd15d7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
FEDORA-2015-ec2ddd15d7

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172647.html

Fedora Core 22

libpng10-1.0.64-1.fc22

91935 - Oracle Enterprise Linux ELSA-2015-2101 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2013-1753, CVE-2014-4616, CVE-2014-4650, CVE-2014-7185

Description

The scan detected that the host is missing the following update:
ELSA-2015-2101

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005559.html

OEL7
x86_64
python-debug-2.7.5-34.0.1.el7
tkinter-2.7.5-34.0.1.el7
python-libs-2.7.5-34.0.1.el7
python-2.7.5-34.0.1.el7
python-test-2.7.5-34.0.1.el7
python-tools-2.7.5-34.0.1.el7
python-devel-2.7.5-34.0.1.el7

91939 - Oracle Enterprise Linux ELSA-2015-2140 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1782

Description

The scan detected that the host is missing the following update:
ELSA-2015-2140

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005554.html

OEL7
x86_64
libssh2-docs-1.4.3-10.el7
libssh2-devel-1.4.3-10.el7
libssh2-1.4.3-10.el7

91942 - Oracle Enterprise Linux ELSA-2015-2231 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9297, CVE-2014-9298, CVE-2014-9750, CVE-2014-9751, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405, CVE-2015-5300, CVE-2015-7704

Description

The scan detected that the host is missing the following update:
ELSA-2015-2231

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005572.html

OEL7
x86_64
ntp-4.2.6p5-22.el7
ntp-perl-4.2.6p5-22.el7
ntpdate-4.2.6p5-22.el7
ntp-doc-4.2.6p5-22.el7
sntp-4.2.6p5-22.el7

91954 - Oracle Enterprise Linux ELSA-2015-2241 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1821, CVE-2015-1822, CVE-2015-1853

Description

The scan detected that the host is missing the following update:
ELSA-2015-2241

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005566.html

OEL7
x86_64
chrony-2.1.1-1.el7

91957 - Oracle Enterprise Linux ELSA-2015-2078 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
ELSA-2015-2078

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005547.html

OEL7
x86_64
postgresql-pltcl-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-upgrade-9.2.14-1.el7_1
postgresql-contrib-9.2.14-1.el7_1
postgresql-plpython-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1
postgresql-server-9.2.14-1.el7_1
postgresql-test-9.2.14-1.el7_1
postgresql-docs-9.2.14-1.el7_1
postgresql-devel-9.2.14-1.el7_1
postgresql-plperl-9.2.14-1.el7_1

91958 - Oracle Enterprise Linux ELSA-2015-2081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288

Description

The scan detected that the host is missing the following update:
ELSA-2015-2081

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005549.html

OEL6
x86_64
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7

postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

i386
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

140976 - Red Hat Enterprise Linux RHSA-2015-2152 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5313, CVE-2013-7421, CVE-2014-3647, CVE-2014-7842, CVE-2014-8171, CVE-2014-9419, CVE-2014-9644, CVE-2015-0239, CVE-2015-2925, CVE-2015-3339, CVE-2015-4170, CVE-2015-5283, CVE-2015-6526, CVE-2015-7613, CVE-2015-7837

Description

The scan detected that the host is missing the following update:
RHSA-2015-2152

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2152.html

RHEL7D
x86_64
kernel-debug-devel-3.10.0-327.el7
python-perf-debuginfo-3.10.0-327.el7
kernel-tools-3.10.0-327.el7
perf-3.10.0-327.el7
kernel-debug-3.10.0-327.el7
kernel-3.10.0-327.el7
python-perf-3.10.0-327.el7
kernel-devel-3.10.0-327.el7
kernel-tools-debuginfo-3.10.0-327.el7
kernel-debug-debuginfo-3.10.0-327.el7
kernel-headers-3.10.0-327.el7
perf-debuginfo-3.10.0-327.el7
kernel-tools-libs-devel-3.10.0-327.el7
kernel-debuginfo-common-x86_64-3.10.0-327.el7
kernel-tools-libs-3.10.0-327.el7
kernel-debuginfo-3.10.0-327.el7

noarch
kernel-abi-whitelists-3.10.0-327.el7
kernel-doc-3.10.0-327.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-327.el7

kernel-doc-3.10.0-327.el7

RHEL7WS
x86_64
kernel-debug-devel-3.10.0-327.el7
python-perf-debuginfo-3.10.0-327.el7
kernel-tools-3.10.0-327.el7
perf-3.10.0-327.el7
kernel-debug-3.10.0-327.el7
kernel-3.10.0-327.el7
python-perf-3.10.0-327.el7
kernel-devel-3.10.0-327.el7
kernel-tools-debuginfo-3.10.0-327.el7
kernel-debug-debuginfo-3.10.0-327.el7
kernel-headers-3.10.0-327.el7
perf-debuginfo-3.10.0-327.el7
kernel-tools-libs-devel-3.10.0-327.el7
kernel-debuginfo-common-x86_64-3.10.0-327.el7
kernel-tools-libs-3.10.0-327.el7
kernel-debuginfo-3.10.0-327.el7

noarch
kernel-abi-whitelists-3.10.0-327.el7
kernel-doc-3.10.0-327.el7

140979 - Red Hat Enterprise Linux RHSA-2015-2081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288

Description

The scan detected that the host is missing the following update:
RHSA-2015-2081

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2081.html

RHEL6D
x86_64
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

i386
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7

postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

RHEL6S
i386
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

x86_64
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

RHEL6WS
x86_64
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

i386
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7

postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

140988 - Red Hat Enterprise Linux RHSA-2015-2140 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1782

Description

The scan detected that the host is missing the following update:
RHSA-2015-2140

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2140.html

RHEL7D
x86_64
libssh2-devel-1.4.3-10.el7
libssh2-debuginfo-1.4.3-10.el7
libssh2-1.4.3-10.el7

noarch
libssh2-docs-1.4.3-10.el7

RHEL7WS
x86_64
libssh2-devel-1.4.3-10.el7
libssh2-debuginfo-1.4.3-10.el7
libssh2-1.4.3-10.el7

noarch
libssh2-docs-1.4.3-10.el7

140990 - Red Hat Enterprise Linux RHSA-2015-2078 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
RHSA-2015-2078

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2078.html

RHEL7D
x86_64

postgresql-pltcl-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-plperl-9.2.14-1.el7_1
postgresql-upgrade-9.2.14-1.el7_1
postgresql-contrib-9.2.14-1.el7_1
postgresql-plpython-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1
postgresql-server-9.2.14-1.el7_1
postgresql-test-9.2.14-1.el7_1
postgresql-docs-9.2.14-1.el7_1
postgresql-devel-9.2.14-1.el7_1
postgresql-debuginfo-9.2.14-1.el7_1

RHEL7S
x86_64
postgresql-pltcl-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-plperl-9.2.14-1.el7_1
postgresql-upgrade-9.2.14-1.el7_1
postgresql-contrib-9.2.14-1.el7_1
postgresql-plpython-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1
postgresql-server-9.2.14-1.el7_1
postgresql-test-9.2.14-1.el7_1
postgresql-docs-9.2.14-1.el7_1
postgresql-devel-9.2.14-1.el7_1
postgresql-debuginfo-9.2.14-1.el7_1

RHEL7WS
x86_64
postgresql-pltcl-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-plperl-9.2.14-1.el7_1
postgresql-upgrade-9.2.14-1.el7_1
postgresql-contrib-9.2.14-1.el7_1
postgresql-plpython-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1
postgresql-server-9.2.14-1.el7_1
postgresql-test-9.2.14-1.el7_1
postgresql-docs-9.2.14-1.el7_1
postgresql-devel-9.2.14-1.el7_1
postgresql-debuginfo-9.2.14-1.el7_1

140998 - Red Hat Enterprise Linux RHSA-2015-2355 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

Description

The scan detected that the host is missing the following update:
RHSA-2015-2355

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2355.html

RHEL7D
x86_64
python-sss-murmur-1.13.0-40.el7
sssd-proxy-1.13.0-40.el7
sssd-1.13.0-40.el7
sssd-ipa-1.13.0-40.el7
python-libsss_nss_idmap-1.13.0-40.el7
sssd-ldap-1.13.0-40.el7
libsss_simpleifp-devel-1.13.0-40.el7
libsss_simpleifp-1.13.0-40.el7
sssd-libwbclient-1.13.0-40.el7
sssd-client-1.13.0-40.el7
libsss_nss_idmap-devel-1.13.0-40.el7
sssd-krb5-common-1.13.0-40.el7
python-sss-1.13.0-40.el7
sssd-debuginfo-1.13.0-40.el7
sssd-common-1.13.0-40.el7
sssd-common-pac-1.13.0-40.el7
sssd-libwbclient-devel-1.13.0-40.el7
libsss_idmap-1.13.0-40.el7
libipa_hbac-1.13.0-40.el7
sssd-dbus-1.13.0-40.el7
python-libipa_hbac-1.13.0-40.el7
libsss_nss_idmap-1.13.0-40.el7
sssd-krb5-1.13.0-40.el7
libsss_idmap-devel-1.13.0-40.el7
libipa_hbac-devel-1.13.0-40.el7
sssd-ad-1.13.0-40.el7
sssd-tools-1.13.0-40.el7

noarch
python-sssdconfig-1.13.0-40.el7

RHEL7WS
x86_64
python-sss-murmur-1.13.0-40.el7
sssd-proxy-1.13.0-40.el7
sssd-1.13.0-40.el7
sssd-ipa-1.13.0-40.el7
python-libsss_nss_idmap-1.13.0-40.el7
sssd-ldap-1.13.0-40.el7
libsss_simpleifp-devel-1.13.0-40.el7
libsss_simpleifp-1.13.0-40.el7
sssd-libwbclient-1.13.0-40.el7
sssd-client-1.13.0-40.el7
libsss_nss_idmap-devel-1.13.0-40.el7
sssd-krb5-common-1.13.0-40.el7
python-sss-1.13.0-40.el7
sssd-debuginfo-1.13.0-40.el7
sssd-common-1.13.0-40.el7
sssd-common-pac-1.13.0-40.el7
sssd-libwbclient-devel-1.13.0-40.el7
libsss_idmap-1.13.0-40.el7
libipa_hbac-1.13.0-40.el7
sssd-dbus-1.13.0-40.el7
python-libipa_hbac-1.13.0-40.el7
libsss_nss_idmap-1.13.0-40.el7
sssd-krb5-1.13.0-40.el7
libsss_idmap-devel-1.13.0-40.el7
libipa_hbac-devel-1.13.0-40.el7

sssd-ad-1.13.0-40.el7
sssd-tools-1.13.0-40.el7

noarch
python-sssdconfig-1.13.0-40.el7

141002 - Red Hat Enterprise Linux RHSA-2015-2083 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
RHSA-2015-2083

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2083.html

RHEL7S
x86_64
postgresql92-postgresql-plperl-9.2.14-1.el7
postgresql92-postgresql-server-9.2.14-1.el7
postgresql92-postgresql-debuginfo-9.2.14-1.el7
postgresql92-postgresql-libs-9.2.14-1.el7
postgresql92-postgresql-pltcl-9.2.14-1.el7
postgresql92-postgresql-docs-9.2.14-1.el7
postgresql92-postgresql-test-9.2.14-1.el7
postgresql92-postgresql-9.2.14-1.el7
postgresql92-postgresql-upgrade-9.2.14-1.el7
postgresql92-postgresql-contrib-9.2.14-1.el7
postgresql92-postgresql-devel-9.2.14-1.el7
postgresql92-postgresql-plpython-9.2.14-1.el7

RHEL6S
x86_64
postgresql92-postgresql-pltcl-9.2.14-1.el6
postgresql92-postgresql-debuginfo-9.2.14-1.el6
postgresql92-postgresql-server-9.2.14-1.el6
postgresql92-postgresql-test-9.2.14-1.el6
postgresql92-postgresql-docs-9.2.14-1.el6
postgresql92-postgresql-plpython-9.2.14-1.el6
postgresql92-postgresql-libs-9.2.14-1.el6
postgresql92-postgresql-contrib-9.2.14-1.el6
postgresql92-postgresql-devel-9.2.14-1.el6
postgresql92-postgresql-plperl-9.2.14-1.el6
postgresql92-postgresql-upgrade-9.2.14-1.el6
postgresql92-postgresql-9.2.14-1.el6

RHEL6WS
x86_64
postgresql92-postgresql-pltcl-9.2.14-1.el6
postgresql92-postgresql-debuginfo-9.2.14-1.el6
postgresql92-postgresql-server-9.2.14-1.el6
postgresql92-postgresql-test-9.2.14-1.el6

postgresql92-postgresql-docs-9.2.14-1.el6
postgresql92-postgresql-plpython-9.2.14-1.el6
postgresql92-postgresql-libs-9.2.14-1.el6
postgresql92-postgresql-contrib-9.2.14-1.el6
postgresql92-postgresql-devel-9.2.14-1.el6
postgresql92-postgresql-plperl-9.2.14-1.el6
postgresql92-postgresql-upgrade-9.2.14-1.el6
postgresql92-postgresql-9.2.14-1.el6

RHEL6_6S
x86_64
postgresql92-postgresql-pltcl-9.2.14-1.el6
postgresql92-postgresql-debuginfo-9.2.14-1.el6
postgresql92-postgresql-server-9.2.14-1.el6
postgresql92-postgresql-test-9.2.14-1.el6
postgresql92-postgresql-docs-9.2.14-1.el6
postgresql92-postgresql-plpython-9.2.14-1.el6
postgresql92-postgresql-libs-9.2.14-1.el6
postgresql92-postgresql-contrib-9.2.14-1.el6
postgresql92-postgresql-devel-9.2.14-1.el6
postgresql92-postgresql-plperl-9.2.14-1.el6
postgresql92-postgresql-upgrade-9.2.14-1.el6
postgresql92-postgresql-9.2.14-1.el6

RHEL6_5S
x86_64
postgresql92-postgresql-pltcl-9.2.14-1.el6
postgresql92-postgresql-debuginfo-9.2.14-1.el6
postgresql92-postgresql-server-9.2.14-1.el6
postgresql92-postgresql-test-9.2.14-1.el6
postgresql92-postgresql-docs-9.2.14-1.el6
postgresql92-postgresql-plpython-9.2.14-1.el6
postgresql92-postgresql-libs-9.2.14-1.el6
postgresql92-postgresql-contrib-9.2.14-1.el6
postgresql92-postgresql-devel-9.2.14-1.el6
postgresql92-postgresql-plperl-9.2.14-1.el6
postgresql92-postgresql-upgrade-9.2.14-1.el6
postgresql92-postgresql-9.2.14-1.el6

RHEL7WS
x86_64
postgresql92-postgresql-plperl-9.2.14-1.el7
postgresql92-postgresql-server-9.2.14-1.el7
postgresql92-postgresql-debuginfo-9.2.14-1.el7
postgresql92-postgresql-libs-9.2.14-1.el7
postgresql92-postgresql-pltcl-9.2.14-1.el7
postgresql92-postgresql-docs-9.2.14-1.el7
postgresql92-postgresql-test-9.2.14-1.el7
postgresql92-postgresql-9.2.14-1.el7
postgresql92-postgresql-upgrade-9.2.14-1.el7
postgresql92-postgresql-contrib-9.2.14-1.el7
postgresql92-postgresql-devel-9.2.14-1.el7
postgresql92-postgresql-plpython-9.2.14-1.el7

141010 - Red Hat Enterprise Linux RHSA-2015-2101 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2013-1753, CVE-2014-4616, CVE-2014-4650, CVE-2014-7185, CVE-2014-9365

Description

The scan detected that the host is missing the following update:
RHSA-2015-2101

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2101.html

RHEL7D
x86_64
python-debuginfo-2.7.5-34.el7
tkinter-2.7.5-34.el7
python-tools-2.7.5-34.el7
python-devel-2.7.5-34.el7
python-test-2.7.5-34.el7
python-libs-2.7.5-34.el7
python-2.7.5-34.el7
python-debug-2.7.5-34.el7

RHEL7WS
x86_64
python-debuginfo-2.7.5-34.el7
tkinter-2.7.5-34.el7
python-tools-2.7.5-34.el7
python-devel-2.7.5-34.el7
python-test-2.7.5-34.el7
python-libs-2.7.5-34.el7
python-2.7.5-34.el7
python-debug-2.7.5-34.el7

141016 - Red Hat Enterprise Linux RHSA-2015-2077 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
RHSA-2015-2077

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2077.html

RHEL7S
x86_64
rh-postgresql94-postgresql-libs-9.4.5-1.el7
rh-postgresql94-postgresql-plperl-9.4.5-1.el7
rh-postgresql94-postgresql-pltcl-9.4.5-1.el7
rh-postgresql94-postgresql-test-9.4.5-1.el7
rh-postgresql94-postgresql-docs-9.4.5-1.el7
rh-postgresql94-postgresql-upgrade-9.4.5-1.el7
rh-postgresql94-postgresql-devel-9.4.5-1.el7

rh-postgresql94-postgresql-plpython-9.4.5-1.el7
rh-postgresql94-postgresql-debuginfo-9.4.5-1.el7
rh-postgresql94-postgresql-9.4.5-1.el7
rh-postgresql94-postgresql-server-9.4.5-1.el7
rh-postgresql94-postgresql-contrib-9.4.5-1.el7

RHEL6S
x86_64
rh-postgresql94-postgresql-9.4.5-1.el6
rh-postgresql94-postgresql-upgrade-9.4.5-1.el6
rh-postgresql94-postgresql-contrib-9.4.5-1.el6
rh-postgresql94-postgresql-devel-9.4.5-1.el6
rh-postgresql94-postgresql-docs-9.4.5-1.el6
rh-postgresql94-postgresql-test-9.4.5-1.el6
rh-postgresql94-postgresql-pltcl-9.4.5-1.el6
rh-postgresql94-postgresql-plpython-9.4.5-1.el6
rh-postgresql94-postgresql-libs-9.4.5-1.el6
rh-postgresql94-postgresql-plperl-9.4.5-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.5-1.el6
rh-postgresql94-postgresql-server-9.4.5-1.el6

RHEL6WS
x86_64
rh-postgresql94-postgresql-9.4.5-1.el6
rh-postgresql94-postgresql-upgrade-9.4.5-1.el6
rh-postgresql94-postgresql-contrib-9.4.5-1.el6
rh-postgresql94-postgresql-devel-9.4.5-1.el6
rh-postgresql94-postgresql-docs-9.4.5-1.el6
rh-postgresql94-postgresql-test-9.4.5-1.el6
rh-postgresql94-postgresql-pltcl-9.4.5-1.el6
rh-postgresql94-postgresql-plpython-9.4.5-1.el6
rh-postgresql94-postgresql-libs-9.4.5-1.el6
rh-postgresql94-postgresql-plperl-9.4.5-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.5-1.el6
rh-postgresql94-postgresql-server-9.4.5-1.el6

RHEL6_6S
x86_64
rh-postgresql94-postgresql-9.4.5-1.el6
rh-postgresql94-postgresql-upgrade-9.4.5-1.el6
rh-postgresql94-postgresql-contrib-9.4.5-1.el6
rh-postgresql94-postgresql-devel-9.4.5-1.el6
rh-postgresql94-postgresql-docs-9.4.5-1.el6
rh-postgresql94-postgresql-test-9.4.5-1.el6
rh-postgresql94-postgresql-pltcl-9.4.5-1.el6
rh-postgresql94-postgresql-plpython-9.4.5-1.el6
rh-postgresql94-postgresql-libs-9.4.5-1.el6
rh-postgresql94-postgresql-plperl-9.4.5-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.5-1.el6
rh-postgresql94-postgresql-server-9.4.5-1.el6

RHEL6_5S
x86_64
rh-postgresql94-postgresql-9.4.5-1.el6
rh-postgresql94-postgresql-upgrade-9.4.5-1.el6
rh-postgresql94-postgresql-contrib-9.4.5-1.el6
rh-postgresql94-postgresql-devel-9.4.5-1.el6
rh-postgresql94-postgresql-docs-9.4.5-1.el6
rh-postgresql94-postgresql-test-9.4.5-1.el6
rh-postgresql94-postgresql-pltcl-9.4.5-1.el6

rh-postgresql94-postgresql-plpython-9.4.5-1.el6
rh-postgresql94-postgresql-libs-9.4.5-1.el6
rh-postgresql94-postgresql-plperl-9.4.5-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.5-1.el6
rh-postgresql94-postgresql-server-9.4.5-1.el6

RHEL7WS
x86_64
rh-postgresql94-postgresql-libs-9.4.5-1.el7
rh-postgresql94-postgresql-plperl-9.4.5-1.el7
rh-postgresql94-postgresql-pltcl-9.4.5-1.el7
rh-postgresql94-postgresql-test-9.4.5-1.el7
rh-postgresql94-postgresql-docs-9.4.5-1.el7
rh-postgresql94-postgresql-upgrade-9.4.5-1.el7
rh-postgresql94-postgresql-devel-9.4.5-1.el7
rh-postgresql94-postgresql-plpython-9.4.5-1.el7
rh-postgresql94-postgresql-debuginfo-9.4.5-1.el7
rh-postgresql94-postgresql-9.4.5-1.el7
rh-postgresql94-postgresql-server-9.4.5-1.el7
rh-postgresql94-postgresql-contrib-9.4.5-1.el7

141017 - Red Hat Enterprise Linux RHSA-2015-2231 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9297, CVE-2014-9298, CVE-2014-9750, CVE-2014-9751, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405

Description

The scan detected that the host is missing the following update:
RHSA-2015-2231

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2231.html

RHEL7D
x86_64
ntp-debuginfo-4.2.6p5-22.el7
ntpdate-4.2.6p5-22.el7
ntp-4.2.6p5-22.el7
sntp-4.2.6p5-22.el7

noarch
ntp-doc-4.2.6p5-22.el7
ntp-perl-4.2.6p5-22.el7

RHEL7WS
x86_64
ntp-debuginfo-4.2.6p5-22.el7
ntpdate-4.2.6p5-22.el7
ntp-4.2.6p5-22.el7
sntp-4.2.6p5-22.el7

noarch
ntp-doc-4.2.6p5-22.el7
ntp-perl-4.2.6p5-22.el7

141018 - Red Hat Enterprise Linux RHSA-2015-2241 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1821, CVE-2015-1822, CVE-2015-1853

Description

The scan detected that the host is missing the following update:
RHSA-2015-2241

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2241.html

RHEL7D
x86_64
chrony-2.1.1-1.el7
chrony-debuginfo-2.1.1-1.el7

RHEL7WS
x86_64
chrony-2.1.1-1.el7
chrony-debuginfo-2.1.1-1.el7

144055 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2070-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-6031

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2070-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00122.html

SuSE Linux 13.1
x86_64
miniupnpc-debuginfo-1.9-2.7.1
python-miniupnpc-debuginfo-1.9-2.7.1
libminiupnpc-devel-1.9-2.7.1
libminiupnpc10-1.9-2.7.1
miniupnpc-1.9-2.7.1
libminiupnpc10-debuginfo-1.9-2.7.1
python-miniupnpc-1.9-2.7.1

i586
miniupnpc-debuginfo-1.9-2.7.1
python-miniupnpc-debuginfo-1.9-2.7.1

libminiupnpc-devel-1.9-2.7.1
libminiupnpc10-1.9-2.7.1
miniupnpc-1.9-2.7.1
libminiupnpc10-debuginfo-1.9-2.7.1
python-miniupnpc-1.9-2.7.1

SuSE Linux 13.2
x86_64
python-miniupnpc-1.9-2.3.1
libminiupnpc10-debuginfo-1.9-2.3.1
libminiupnpc10-1.9-2.3.1
libminiupnpc-devel-1.9-2.3.1
miniupnpc-debuginfo-1.9-2.3.1
python-miniupnpc-debuginfo-1.9-2.3.1
miniupnpc-1.9-2.3.1

i586
python-miniupnpc-1.9-2.3.1
libminiupnpc10-debuginfo-1.9-2.3.1
libminiupnpc10-1.9-2.3.1
libminiupnpc-devel-1.9-2.3.1
miniupnpc-debuginfo-1.9-2.3.1
python-miniupnpc-debuginfo-1.9-2.3.1
miniupnpc-1.9-2.3.1

160001 - CentOS 6 CESA-2015-2081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288

Description

The scan detected that the host is missing the following update:
CESA-2015-2081

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021504.html

CentOS 6
x86_64
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

i686
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7

postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

160003 - CentOS 7 CESA-2015-2078 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
CESA-2015-2078

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021508.html

CentOS 7
x86_64
postgresql-pltcl-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-upgrade-9.2.14-1.el7_1
postgresql-contrib-9.2.14-1.el7_1
postgresql-plpython-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1
postgresql-server-9.2.14-1.el7_1
postgresql-test-9.2.14-1.el7_1
postgresql-docs-9.2.14-1.el7_1
postgresql-devel-9.2.14-1.el7_1
postgresql-plperl-9.2.14-1.el7_1

i686
postgresql-devel-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1

181685 - FreeBSD libxml2 Multiple Vulnabilities (e5423caf-8fb8-11e5-918c-bcaec565249c)

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

Risk Level: Medium

CVE: CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8035, CVE-2015-8241, CVE-2015-8242

Description

The scan detected that the host is missing the following update:
libxml2 -- multiple vulnabilities (e5423caf-8fb8-11e5-918c-bcaec565249c)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/e5423caf-8fb8-11e5-918c-bcaec565249c.html

Affected packages:
libxml2 < 2.9.3

185060 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2817-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5234, CVE-2015-5235

Description

The scan detected that the host is missing the following update:
USN-2817-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003199.html

Ubuntu 15.04

icedtea-7-plugin_1.5.3-0ubuntu0.15.04.1

Ubuntu 15.10

icedtea-7-plugin_1.5.3-0ubuntu0.15.10.1

Ubuntu 14.04

icedtea-6-plugin_1.5.3-0ubuntu0.14.04.1
icedtea-7-plugin_1.5.3-0ubuntu0.14.04.1

185063 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2814-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7869

Description

The scan detected that the host is missing the following update:
USN-2814-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003196.html

Ubuntu 12.04

nvidia-304_304.131-0ubuntu0.12.04.1
nvidia-340-updates_340.96-0ubuntu0.12.04.1

nvidia-304-updates_304.131-0ubuntu0.12.04.1
nvidia-340_340.96-0ubuntu0.12.04.1
nvidia-331-updates_340.96-0ubuntu0.12.04.1

Ubuntu 15.04

nvidia-352-updates_352.63-0ubuntu0.15.04.1
nvidia-340-updates_340.96-0ubuntu0.15.04.1
nvidia-304_304.131-0ubuntu0.15.04.1
nvidia-352_352.63-0ubuntu0.15.04.1
nvidia-340_340.96-0ubuntu0.15.04.1
nvidia-304-updates_304.131-0ubuntu0.15.04.1
nvidia-346_352.63-0ubuntu0.15.04.1
nvidia-331-updates_340.96-0ubuntu0.15.04.1
nvidia-346-updates_352.63-0ubuntu0.15.04.1
nvidia-331_340.96-0ubuntu0.15.04.1

Ubuntu 15.10

nvidia-346-updates_352.63-0ubuntu0.15.10.1
nvidia-340_340.96-0ubuntu0.15.10.1
nvidia-352_352.63-0ubuntu0.15.10.1
nvidia-331_340.96-0ubuntu0.15.10.1
nvidia-352-updates_352.63-0ubuntu0.15.10.1
nvidia-304_304.131-0ubuntu0.15.10.1
nvidia-346_352.63-0ubuntu0.15.10.1
nvidia-331-updates_340.96-0ubuntu0.15.10.1
nvidia-304-updates_304.131-0ubuntu0.15.10.1
nvidia-340-updates_340.96-0ubuntu0.15.10.1

Ubuntu 14.04

nvidia-346-updates_352.63-0ubuntu0.14.04.1
nvidia-304-updates_304.131-0ubuntu0.14.04.1
nvidia-304_304.131-0ubuntu0.14.04.1
nvidia-331_340.96-0ubuntu0.14.04.1
nvidia-340-updates_340.96-0ubuntu0.14.04.1
nvidia-346_352.63-0ubuntu0.14.04.1
nvidia-331-updates_340.96-0ubuntu0.14.04.1
nvidia-340_340.96-0ubuntu0.14.04.1
nvidia-352-updates_352.63-0ubuntu0.14.04.1
nvidia-352_352.63-0ubuntu0.14.04.1

190007 - Fedora Linux 22 FEDORA-2015-6d2a957a87 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
FEDORA-2015-6d2a957a87

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172316.html

Fedora Core 22

postgresql-9.4.5-1.fc22

19312 - (APSB15-29) Vulnerabilities In Adobe ColdFusion

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

Risk Level: Medium

CVE: CVE-2015-5255, CVE-2015-8052, CVE-2015-8053

Description

Multiple vulnerabilities are present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

Multiple vulnerabilities are present in some versions of Adobe ColdFusion. The flaws are due to improper validation of input data. Successful exploitation could allow an attacker to conduct reflected cross-site scripting attacks or server-side request forgery attack.

The update provided by Adobe bulletin APSB15-29 resolves this issues. The target system appears to be missing this update.

19318 - (VMSA-2015-0008) VMware Horizon View Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-3269

Description

An information disclosure is present in some versions of VMware Horizon View.

Observation

VMware Horizon View is VMware desktop-virtualization product.

An information disclosure is present in some versions of VMware Horizon View. The flaw lies in Apache Flex BlazeDS. Successful exploitation could allow an attacker to read arbitrary files.

19323 - (VMSA-2015-0008) VMware vCenter Server Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-3269

Description

An information disclosure vulnerability is present in some versions of VMware vCenter Server.

Observation

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

An information disclosure vulnerability is present in some versions of VMware vCenter Server. The flaw lies within the Apache Flex BlazeDS. Successful exploitation could allow an attacker to read arbitrary files.

19324 - (VMSA-2015-0008) VMware vCenter Server Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-3269

Description

An information disclosure vulnerability is present in some versions of VMware vCenter Server.

Observation

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

An information disclosure vulnerability is present in some versions of VMware vCenter Server. The flaw lies within the Apache Flex BlazeDS. Successful exploitation could allow an attacker to read arbitrary files.

91933 - Oracle Enterprise Linux ELSA-2015-2151 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2150

Description

The scan detected that the host is missing the following update:
ELSA-2015-2151

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005556.html

OEL7
x86_64
xfsprogs-3.2.2-2.el7
xfsprogs-devel-3.2.2-2.el7
xfsprogs-qa-devel-3.2.2-2.el7

91934 - Oracle Enterprise Linux ELSA-2015-2131 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3276

Description

The scan detected that the host is missing the following update:
ELSA-2015-2131

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005558.html

OEL7
x86_64
openldap-2.4.40-8.el7
openldap-devel-2.4.40-8.el7
openldap-servers-2.4.40-8.el7
openldap-clients-2.4.40-8.el7
openldap-servers-sql-2.4.40-8.el7

91938 - Oracle Enterprise Linux ELSA-2015-2345 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3565

Description

The scan detected that the host is missing the following update:
ELSA-2015-2345

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005565.html

OEL7
x86_64
net-snmp-libs-5.7.2-24.el7
net-snmp-perl-5.7.2-24.el7
net-snmp-utils-5.7.2-24.el7
net-snmp-agent-libs-5.7.2-24.el7
net-snmp-sysvinit-5.7.2-24.el7
net-snmp-devel-5.7.2-24.el7
net-snmp-5.7.2-24.el7
net-snmp-gui-5.7.2-24.el7
net-snmp-python-5.7.2-24.el7

91941 - Oracle Enterprise Linux ELSA-2015-2180 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0334

Description

The scan detected that the host is missing the following update:
ELSA-2015-2180

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005563.html

OEL7
x86_64
rubygem-thor-doc-0.19.1-1.el7
rubygem-bundler-doc-1.7.8-3.el7

rubygem-bundler-1.7.8-3.el7
rubygem-thor-0.19.1-1.el7

91946 - Oracle Enterprise Linux ELSA-2015-2159 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, CVE-2015-3148

Description

The scan detected that the host is missing the following update:
ELSA-2015-2159

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005564.html

OEL7
x86_64
curl-7.29.0-25.0.1.el7
libcurl-7.29.0-25.0.1.el7
libcurl-devel-7.29.0-25.0.1.el7

91948 - Oracle Enterprise Linux ELSA-2015-2248 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Description

The scan detected that the host is missing the following update:
ELSA-2015-2248

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005561.html

OEL7
x86_64
netcf-libs-0.2.8-1.el7
netcf-devel-0.2.8-1.el7
netcf-0.2.8-1.el7

91950 - Oracle Enterprise Linux ELSA-2015-2504 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5302

Description

The scan detected that the host is missing the following update:
ELSA-2015-2504

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005552.html

OEL6
x86_64
libreport-plugin-ureport-2.0.9-25.0.1.el6_7
libreport-devel-2.0.9-25.0.1.el6_7
libreport-python-2.0.9-25.0.1.el6_7
libreport-plugin-reportuploader-2.0.9-25.0.1.el6_7
libreport-plugin-kerneloops-2.0.9-25.0.1.el6_7
libreport-filesystem-2.0.9-25.0.1.el6_7
libreport-gtk-devel-2.0.9-25.0.1.el6_7
libreport-plugin-bugzilla-2.0.9-25.0.1.el6_7
libreport-plugin-mailx-2.0.9-25.0.1.el6_7
libreport-gtk-2.0.9-25.0.1.el6_7
libreport-compat-2.0.9-25.0.1.el6_7
libreport-plugin-logger-2.0.9-25.0.1.el6_7
libreport-2.0.9-25.0.1.el6_7
libreport-cli-2.0.9-25.0.1.el6_7
libreport-newt-2.0.9-25.0.1.el6_7

i386
libreport-plugin-ureport-2.0.9-25.0.1.el6_7
libreport-devel-2.0.9-25.0.1.el6_7
libreport-python-2.0.9-25.0.1.el6_7
libreport-plugin-reportuploader-2.0.9-25.0.1.el6_7
libreport-plugin-kerneloops-2.0.9-25.0.1.el6_7
libreport-filesystem-2.0.9-25.0.1.el6_7
libreport-gtk-devel-2.0.9-25.0.1.el6_7
libreport-plugin-bugzilla-2.0.9-25.0.1.el6_7
libreport-plugin-mailx-2.0.9-25.0.1.el6_7
libreport-gtk-2.0.9-25.0.1.el6_7
libreport-compat-2.0.9-25.0.1.el6_7
libreport-plugin-logger-2.0.9-25.0.1.el6_7
libreport-2.0.9-25.0.1.el6_7
libreport-cli-2.0.9-25.0.1.el6_7
libreport-newt-2.0.9-25.0.1.el6_7

91951 - Oracle Enterprise Linux ELSA-2015-2154 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-5355, CVE-2015-2694

Description

The scan detected that the host is missing the following update:
ELSA-2015-2154

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005557.html

OEL7
x86_64
krb5-server-ldap-1.13.2-10.el7
krb5-workstation-1.13.2-10.el7
krb5-server-1.13.2-10.el7
krb5-devel-1.13.2-10.el7
krb5-pkinit-1.13.2-10.el7
krb5-libs-1.13.2-10.el7

91955 - Oracle Enterprise Linux ELSA-2015-2108 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9112

Description

The scan detected that the host is missing the following update:
ELSA-2015-2108

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005553.html

OEL7
x86_64
cpio-2.11-24.el7

130320 - Debian Linux 7.0, 8.0 DSA-3401-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4871

Description

The scan detected that the host is missing the following update:
DSA-3401-1

Observation

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

http://www.debian.org/security/2015/dsa-3401

Debian 8.0
all
openjdk-7-source_7u91-2.6.3-1~deb8u1
openjdk-7-jre_7u91-2.6.3-1~deb8u1
openjdk-7-jdk_7u91-2.6.3-1~deb8u1
openjdk-7-dbg_7u91-2.6.3-1~deb8u1
openjdk-7-jre-lib_7u91-2.6.3-1~deb8u1
icedtea-7-jre-jamvm_7u91-2.6.3-1~deb8u1
openjdk-7-doc_7u91-2.6.3-1~deb8u1

openjdk-7-jre-headless_7u91-2.6.3-1~deb8u1
openjdk-7-demo_7u91-2.6.3-1~deb8u1
openjdk-7-jre-zero_7u91-2.6.3-1~deb8u1

Debian 7.0
all
icedtea-7-jre-jamvm_7u91-2.6.3-1~deb7u1
openjdk-7-demo_7u91-2.6.3-1~deb7u1
openjdk-7-doc_7u91-2.6.3-1~deb7u1
openjdk-7-jre-headless_7u91-2.6.3-1~deb7u1
icedtea-7-jre-cacao_7u91-2.6.3-1~deb7u1
openjdk-7-jre-zero_7u91-2.6.3-1~deb7u1
openjdk-7-jdk_7u91-2.6.3-1~deb7u1
openjdk-7-jre_7u91-2.6.3-1~deb7u1
openjdk-7-jre-lib_7u91-2.6.3-1~deb7u1
openjdk-7-source_7u91-2.6.3-1~deb7u1
openjdk-7-dbg_7u91-2.6.3-1~deb7u1

140980 - Red Hat Enterprise Linux RHSA-2015-2159 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, CVE-2015-3148

Description

The scan detected that the host is missing the following update:
RHSA-2015-2159

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2159.html

RHEL7D
x86_64
curl-debuginfo-7.29.0-25.el7
libcurl-devel-7.29.0-25.el7
libcurl-7.29.0-25.el7
curl-7.29.0-25.el7

RHEL7WS
x86_64
curl-debuginfo-7.29.0-25.el7
libcurl-devel-7.29.0-25.el7
libcurl-7.29.0-25.el7
curl-7.29.0-25.el7

140986 - Red Hat Enterprise Linux RHSA-2015-2248 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Description

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

RHSA-2015-2248

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2248.html

RHEL7D
x86_64
netcf-devel-0.2.8-1.el7
netcf-debuginfo-0.2.8-1.el7
netcf-0.2.8-1.el7
netcf-libs-0.2.8-1.el7

RHEL7S
ppc64
netcf-devel-0.2.8-1.el7
netcf-debuginfo-0.2.8-1.el7
netcf-0.2.8-1.el7
netcf-libs-0.2.8-1.el7

RHEL7WS
x86_64
netcf-devel-0.2.8-1.el7
netcf-debuginfo-0.2.8-1.el7
netcf-0.2.8-1.el7
netcf-libs-0.2.8-1.el7

140989 - Red Hat Enterprise Linux RHSA-2015-2180 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0334

Description

The scan detected that the host is missing the following update:
RHSA-2015-2180

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2180.html

RHEL7D
noarch
rubygem-thor-doc-0.19.1-1.el7
rubygem-bundler-doc-1.7.8-3.el7
rubygem-bundler-1.7.8-3.el7
rubygem-thor-0.19.1-1.el7

RHEL7S
noarch
rubygem-thor-doc-0.19.1-1.el7
rubygem-bundler-doc-1.7.8-3.el7
rubygem-bundler-1.7.8-3.el7

rubygem-thor-0.19.1-1.el7

RHEL7WS
noarch
rubygem-thor-doc-0.19.1-1.el7
rubygem-bundler-doc-1.7.8-3.el7
rubygem-bundler-1.7.8-3.el7
rubygem-thor-0.19.1-1.el7

140995 - Red Hat Enterprise Linux RHSA-2015-2154 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-5355, CVE-2015-2694

Description

The scan detected that the host is missing the following update:
RHSA-2015-2154

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2154.html

RHEL7D
x86_64
krb5-server-ldap-1.13.2-10.el7
krb5-workstation-1.13.2-10.el7
krb5-server-1.13.2-10.el7
krb5-devel-1.13.2-10.el7
krb5-pkinit-1.13.2-10.el7
krb5-libs-1.13.2-10.el7
krb5-debuginfo-1.13.2-10.el7

RHEL7WS
x86_64
krb5-server-ldap-1.13.2-10.el7
krb5-workstation-1.13.2-10.el7
krb5-server-1.13.2-10.el7
krb5-devel-1.13.2-10.el7
krb5-pkinit-1.13.2-10.el7
krb5-libs-1.13.2-10.el7
krb5-debuginfo-1.13.2-10.el7

140997 - Red Hat Enterprise Linux RHSA-2015-2315 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0272, CVE-2015-2924

Description

The scan detected that the host is missing the following update:
RHSA-2015-2315

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2315.html

RHEL7D
x86_64
NetworkManager-libreswan-gnome-1.0.6-3.el7
NetworkManager-libreswan-1.0.6-3.el7
ModemManager-glib-1.1.0-8.git20130913.el7
libnm-gtk-1.0.6-2.el7
nm-connection-editor-1.0.6-2.el7
NetworkManager-wwan-1.0.6-27.el7
NetworkManager-1.0.6-27.el7
NetworkManager-libnm-1.0.6-27.el7
ModemManager-glib-devel-1.1.0-8.git20130913.el7
NetworkManager-glib-devel-1.0.6-27.el7
NetworkManager-config-routing-rules-1.0.6-27.el7
ModemManager-debuginfo-1.1.0-8.git20130913.el7
NetworkManager-libreswan-debuginfo-1.0.6-3.el7
network-manager-applet-1.0.6-2.el7
NetworkManager-tui-1.0.6-27.el7
NetworkManager-config-server-1.0.6-27.el7
NetworkManager-devel-1.0.6-27.el7
libnm-gtk-devel-1.0.6-2.el7
NetworkManager-bluetooth-1.0.6-27.el7
NetworkManager-libnm-devel-1.0.6-27.el7
network-manager-applet-debuginfo-1.0.6-2.el7
NetworkManager-glib-1.0.6-27.el7
ModemManager-1.1.0-8.git20130913.el7
NetworkManager-team-1.0.6-27.el7
NetworkManager-adsl-1.0.6-27.el7
ModemManager-vala-1.1.0-8.git20130913.el7
NetworkManager-wifi-1.0.6-27.el7
NetworkManager-debuginfo-1.0.6-27.el7
ModemManager-devel-1.1.0-8.git20130913.el7

RHEL7WS
x86_64
NetworkManager-libreswan-gnome-1.0.6-3.el7
NetworkManager-libreswan-1.0.6-3.el7
ModemManager-glib-1.1.0-8.git20130913.el7
libnm-gtk-1.0.6-2.el7
nm-connection-editor-1.0.6-2.el7
NetworkManager-wwan-1.0.6-27.el7
NetworkManager-1.0.6-27.el7
NetworkManager-libnm-1.0.6-27.el7
ModemManager-glib-devel-1.1.0-8.git20130913.el7
NetworkManager-glib-devel-1.0.6-27.el7
NetworkManager-config-routing-rules-1.0.6-27.el7
ModemManager-debuginfo-1.1.0-8.git20130913.el7
NetworkManager-libreswan-debuginfo-1.0.6-3.el7
network-manager-applet-1.0.6-2.el7
NetworkManager-tui-1.0.6-27.el7
NetworkManager-config-server-1.0.6-27.el7
NetworkManager-devel-1.0.6-27.el7
libnm-gtk-devel-1.0.6-2.el7
NetworkManager-bluetooth-1.0.6-27.el7
NetworkManager-libnm-devel-1.0.6-27.el7
network-manager-applet-debuginfo-1.0.6-2.el7

NetworkManager-glib-1.0.6-27.el7
ModemManager-1.1.0-8.git20130913.el7
NetworkManager-team-1.0.6-27.el7
NetworkManager-adsl-1.0.6-27.el7
ModemManager-vala-1.1.0-8.git20130913.el7
NetworkManager-wifi-1.0.6-27.el7
NetworkManager-debuginfo-1.0.6-27.el7
ModemManager-devel-1.1.0-8.git20130913.el7

140999 - Red Hat Enterprise Linux RHSA-2015-2345 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3565

Description

The scan detected that the host is missing the following update:
RHSA-2015-2345

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2345.html

RHEL7D
x86_64
net-snmp-libs-5.7.2-24.el7
net-snmp-utils-5.7.2-24.el7
net-snmp-agent-libs-5.7.2-24.el7
net-snmp-sysvinit-5.7.2-24.el7
net-snmp-devel-5.7.2-24.el7
net-snmp-perl-5.7.2-24.el7
net-snmp-5.7.2-24.el7
net-snmp-gui-5.7.2-24.el7
net-snmp-debuginfo-5.7.2-24.el7
net-snmp-python-5.7.2-24.el7

RHEL7WS
x86_64
net-snmp-libs-5.7.2-24.el7
net-snmp-utils-5.7.2-24.el7
net-snmp-agent-libs-5.7.2-24.el7
net-snmp-sysvinit-5.7.2-24.el7
net-snmp-devel-5.7.2-24.el7
net-snmp-perl-5.7.2-24.el7
net-snmp-5.7.2-24.el7
net-snmp-gui-5.7.2-24.el7
net-snmp-debuginfo-5.7.2-24.el7
net-snmp-python-5.7.2-24.el7

141000 - Red Hat Enterprise Linux RHSA-2015-2184 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2704

Description

The scan detected that the host is missing the following update:
RHSA-2015-2184

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2184.html

RHEL7D
x86_64
realmd-devel-docs-0.16.1-5.el7
realmd-debuginfo-0.16.1-5.el7
realmd-0.16.1-5.el7

RHEL7WS
x86_64
realmd-devel-docs-0.16.1-5.el7
realmd-debuginfo-0.16.1-5.el7
realmd-0.16.1-5.el7

141001 - Red Hat Enterprise Linux RHSA-2015-2108 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9112

Description

The scan detected that the host is missing the following update:
RHSA-2015-2108

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2108.html

RHEL7D
x86_64
cpio-debuginfo-2.11-24.el7
cpio-2.11-24.el7

RHEL7WS
x86_64
cpio-debuginfo-2.11-24.el7
cpio-2.11-24.el7

141008 - Red Hat Enterprise Linux RHSA-2015-2504 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5302

Description

The scan detected that the host is missing the following update:
RHSA-2015-2504

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2504.html

RHEL6D
x86_64
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-plugin-bugzilla-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-devel-2.0.9-25.el6_7
libreport-gtk-devel-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

i386
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-plugin-bugzilla-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-devel-2.0.9-25.el6_7
libreport-gtk-devel-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

RHEL6S
i386
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-plugin-bugzilla-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7

libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-devel-2.0.9-25.el6_7
libreport-gtk-devel-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

x86_64
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-plugin-bugzilla-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-devel-2.0.9-25.el6_7
libreport-gtk-devel-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

RHEL6WS
x86_64
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

i386
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

141011 - Red Hat Enterprise Linux RHSA-2015-2131 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3276

Description

The scan detected that the host is missing the following update:
RHSA-2015-2131

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2131.html

RHEL7D
x86_64
openldap-servers-2.4.40-8.el7
openldap-servers-sql-2.4.40-8.el7
openldap-2.4.40-8.el7
openldap-debuginfo-2.4.40-8.el7
openldap-clients-2.4.40-8.el7
openldap-devel-2.4.40-8.el7

RHEL7WS
x86_64
openldap-servers-2.4.40-8.el7
openldap-servers-sql-2.4.40-8.el7
openldap-2.4.40-8.el7
openldap-debuginfo-2.4.40-8.el7
openldap-clients-2.4.40-8.el7
openldap-devel-2.4.40-8.el7

141012 - Red Hat Enterprise Linux RHSA-2015-2151 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2150

Description

The scan detected that the host is missing the following update:
RHSA-2015-2151

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2151.html

RHEL7D
x86_64
xfsprogs-3.2.2-2.el7
xfsprogs-devel-3.2.2-2.el7
xfsprogs-qa-devel-3.2.2-2.el7
xfsprogs-debuginfo-3.2.2-2.el7

RHEL7WS
x86_64
xfsprogs-3.2.2-2.el7
xfsprogs-devel-3.2.2-2.el7
xfsprogs-qa-devel-3.2.2-2.el7
xfsprogs-debuginfo-3.2.2-2.el7

141014 - Red Hat Enterprise Linux RHSA-2015-2505 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5273, CVE-2015-5287, CVE-2015-5302

Description

The scan detected that the host is missing the following update:
RHSA-2015-2505

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2505.html

RHEL7D
x86_64
abrt-addon-upload-watch-2.1.11-35.el7
abrt-gui-2.1.11-35.el7
libreport-newt-2.1.11-31.el7
abrt-debuginfo-2.1.11-35.el7
libreport-rhel-2.1.11-31.el7
abrt-addon-xorg-2.1.11-35.el7
libreport-web-2.1.11-31.el7
libreport-python-2.1.11-31.el7
abrt-desktop-2.1.11-35.el7
abrt-addon-kerneloops-2.1.11-35.el7
abrt-addon-python-2.1.11-35.el7
abrt-addon-ccpp-2.1.11-35.el7
libreport-anaconda-2.1.11-31.el7
libreport-compat-2.1.11-31.el7
libreport-plugin-rhtsupport-2.1.11-31.el7
libreport-devel-2.1.11-31.el7
libreport-plugin-reportuploader-2.1.11-31.el7
libreport-rhel-bugzilla-2.1.11-31.el7
libreport-gtk-devel-2.1.11-31.el7
libreport-plugin-mailx-2.1.11-31.el7
libreport-plugin-ureport-2.1.11-31.el7
abrt-devel-2.1.11-35.el7
libreport-2.1.11-31.el7
libreport-debuginfo-2.1.11-31.el7
libreport-web-devel-2.1.11-31.el7
abrt-console-notification-2.1.11-35.el7
abrt-2.1.11-35.el7
libreport-cli-2.1.11-31.el7
abrt-addon-pstoreoops-2.1.11-35.el7
libreport-gtk-2.1.11-31.el7
abrt-gui-devel-2.1.11-35.el7
abrt-dbus-2.1.11-35.el7
abrt-libs-2.1.11-35.el7

abrt-python-2.1.11-35.el7
libreport-plugin-logger-2.1.11-31.el7
libreport-plugin-kerneloops-2.1.11-31.el7
abrt-retrace-client-2.1.11-35.el7
abrt-gui-libs-2.1.11-35.el7
libreport-rhel-anaconda-bugzilla-2.1.11-31.el7
abrt-cli-2.1.11-35.el7
libreport-plugin-bugzilla-2.1.11-31.el7
abrt-tui-2.1.11-35.el7
libreport-filesystem-2.1.11-31.el7
abrt-addon-vmcore-2.1.11-35.el7

noarch
abrt-python-doc-2.1.11-35.el7

RHEL7WS
x86_64
abrt-addon-upload-watch-2.1.11-35.el7
abrt-gui-2.1.11-35.el7
libreport-newt-2.1.11-31.el7
abrt-debuginfo-2.1.11-35.el7
libreport-rhel-2.1.11-31.el7
abrt-addon-xorg-2.1.11-35.el7
libreport-web-2.1.11-31.el7
libreport-python-2.1.11-31.el7
abrt-desktop-2.1.11-35.el7
abrt-addon-kerneloops-2.1.11-35.el7
abrt-addon-python-2.1.11-35.el7
abrt-addon-ccpp-2.1.11-35.el7
libreport-anaconda-2.1.11-31.el7
libreport-compat-2.1.11-31.el7
libreport-plugin-rhtsupport-2.1.11-31.el7
libreport-devel-2.1.11-31.el7
libreport-plugin-reportuploader-2.1.11-31.el7
libreport-rhel-bugzilla-2.1.11-31.el7
libreport-gtk-devel-2.1.11-31.el7
libreport-plugin-mailx-2.1.11-31.el7
libreport-plugin-ureport-2.1.11-31.el7
abrt-devel-2.1.11-35.el7
libreport-2.1.11-31.el7
libreport-debuginfo-2.1.11-31.el7
libreport-web-devel-2.1.11-31.el7
abrt-console-notification-2.1.11-35.el7
abrt-2.1.11-35.el7
libreport-cli-2.1.11-31.el7
abrt-addon-pstoreoops-2.1.11-35.el7
libreport-gtk-2.1.11-31.el7
abrt-gui-devel-2.1.11-35.el7
abrt-dbus-2.1.11-35.el7
abrt-libs-2.1.11-35.el7
abrt-python-2.1.11-35.el7
libreport-plugin-logger-2.1.11-31.el7
libreport-plugin-kerneloops-2.1.11-31.el7
abrt-retrace-client-2.1.11-35.el7
abrt-gui-libs-2.1.11-35.el7
libreport-rhel-anaconda-bugzilla-2.1.11-31.el7
abrt-cli-2.1.11-35.el7
libreport-plugin-bugzilla-2.1.11-31.el7
abrt-tui-2.1.11-35.el7
libreport-filesystem-2.1.11-31.el7

abrt-addon-vmcore-2.1.11-35.el7

noarch
abrt-python-doc-2.1.11-35.el7

181682 - FreeBSD libxslt DoS Vulnability Due To Type Confusing Error (ecc268f2-8fc2-11e5-918c-bcaec565249c)

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

Risk Level: Medium

CVE: CVE-2015-7995

Description

The scan detected that the host is missing the following update:
libxslt -- DoS vulnability due to type confusing error (ecc268f2-8fc2-11e5-918c-bcaec565249c)

Observation

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

http://www.vuxml.org/freebsd/ecc268f2-8fc2-11e5-918c-bcaec565249c.html

Affected packages:
libsxlt < 1.1.28_8

190000 - Fedora Linux 22 FEDORA-2015-992342e82f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0852

Description

The scan detected that the host is missing the following update:
FEDORA-2015-992342e82f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172583.html

Fedora Core 22

mingw-freeimage-3.15.4-6.fc22

190009 - Fedora Linux 21 FEDORA-2015-14200 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5185

Description

The scan detected that the host is missing the following update:
FEDORA-2015-14200

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172667.html

Fedora Core 21

sblim-sfcb-1.4.8-5.fc21

190019 - Fedora Linux 23 FEDORA-2015-14197 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5185

Description

The scan detected that the host is missing the following update:
FEDORA-2015-14197

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172634.html

Fedora Core 23

sblim-sfcb-1.4.9-4.fc23

190020 - Fedora Linux 22 FEDORA-2015-14199 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5185

Description

The scan detected that the host is missing the following update:
FEDORA-2015-14199

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172659.html

Fedora Core 22

sblim-sfcb-1.4.9-2.fc22

190029 - Fedora Linux 22 FEDORA-2015-9eee2fbc78 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7236

Description

The scan detected that the host is missing the following update:
FEDORA-2015-9eee2fbc78

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172152.html

Fedora Core 22

rpcbind-0.2.3-0.3.fc22

190031 - Fedora Linux 23 FEDORA-2015-decbab7c9f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0852

Description

The scan detected that the host is missing the following update:
FEDORA-2015-decbab7c9f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172491.html

Fedora Core 23

mingw-freeimage-3.17.0-1.fc23

190043 - Fedora Linux 21 FEDORA-2015-a3965fd800 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5311

Description

The scan detected that the host is missing the following update:
FEDORA-2015-a3965fd800

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172193.html

Fedora Core 21

pdns-3.4.7-1.fc21

91943 - Oracle Enterprise Linux ELSA-2015-2455 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8602

Description

The scan detected that the host is missing the following update:
ELSA-2015-2455

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005573.html

OEL7
x86_64
unbound-1.4.20-26.el7
unbound-python-1.4.20-26.el7
unbound-libs-1.4.20-26.el7
unbound-devel-1.4.20-26.el7

91945 - Oracle Enterprise Linux ELSA-2015-2417 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8169

Description

The scan detected that the host is missing the following update:
ELSA-2015-2417

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005574.html

OEL7
x86_64
autofs-5.0.7-54.0.1.el7

140987 - Red Hat Enterprise Linux RHSA-2015-2455 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8602

Description

The scan detected that the host is missing the following update:
RHSA-2015-2455

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2455.html

RHEL7D
x86_64
unbound-debuginfo-1.4.20-26.el7
unbound-libs-1.4.20-26.el7
unbound-python-1.4.20-26.el7
unbound-1.4.20-26.el7
unbound-devel-1.4.20-26.el7

RHEL7WS
x86_64
unbound-debuginfo-1.4.20-26.el7
unbound-libs-1.4.20-26.el7
unbound-python-1.4.20-26.el7
unbound-1.4.20-26.el7
unbound-devel-1.4.20-26.el7

141003 - Red Hat Enterprise Linux RHSA-2015-2417 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8169

Description

The scan detected that the host is missing the following update:
RHSA-2015-2417

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2417.html

RHEL7D
x86_64
autofs-5.0.7-54.el7
autofs-debuginfo-5.0.7-54.el7

RHEL7WS
x86_64
autofs-5.0.7-54.el7
autofs-debuginfo-5.0.7-54.el7

189997 - Fedora Linux 22 FEDORA-2015-cd94ad8d7c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-7799, CVE-2015-7990, CVE-2015-8104

Description

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

FEDORA-2015-cd94ad8d7c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172100.html

Fedora Core 22

kernel-4.2.6-200.fc22

190005 - Fedora Linux 22 FEDORA-2015-668d213dc3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
FEDORA-2015-668d213dc3

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172300.html

Fedora Core 22

xen-4.5.2-2.fc22

190011 - Fedora Linux 22 FEDORA-2015-1521e91178 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4142

Description

The scan detected that the host is missing the following update:
FEDORA-2015-1521e91178

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172655.html

Fedora Core 22

wpa_supplicant-2.4-7.fc22

190018 - Fedora Linux 23 FEDORA-2015-394835a3f6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
FEDORA-2015-394835a3f6

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172435.html

Fedora Core 23

xen-4.5.2-2.fc23

190026 - Fedora Linux 21 FEDORA-2015-cfea96144a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4142

Description

The scan detected that the host is missing the following update:
FEDORA-2015-cfea96144a

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172608.html

Fedora Core 21

wpa_supplicant-2.0-17.fc21

190028 - Fedora Linux 21 FEDORA-2015-f150b2a8c8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
FEDORA-2015-f150b2a8c8

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172187.html

Fedora Core 21

xen-4.4.3-8.fc21

190033 - Fedora Linux 23 FEDORA-2015-115c302856 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-7799, CVE-2015-7990, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
FEDORA-2015-115c302856

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172022.html

Fedora Core 23

kernel-4.2.6-300.fc23

190034 - Fedora Linux 21 FEDORA-2015-f2c534bc12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-7799, CVE-2015-7990, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
FEDORA-2015-f2c534bc12

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172185.html

Fedora Core 21

kernel-4.1.13-100.fc21

190041 - Fedora Linux 21 FEDORA-2015-a275fd68f2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-4000, CVE-2015-6566

Description

The scan detected that the host is missing the following update:
FEDORA-2015-a275fd68f2

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172605.html

Fedora Core 21

zarafa-7.1.14-1.fc21

91932 - Oracle Enterprise Linux ELSA-2015-2369 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3248

Description

The scan detected that the host is missing the following update:
ELSA-2015-2369

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005568.html

OEL7
x86_64
openhpi-devel-3.4.0-2.el7
openhpi-3.4.0-2.el7
openhpi-libs-3.4.0-2.el7

91956 - Oracle Enterprise Linux ELSA-2015-2237 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2675

Description

The scan detected that the host is missing the following update:
ELSA-2015-2237

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005567.html

OEL7
x86_64
rest-devel-0.7.92-3.el7
rest-0.7.92-3.el7

130319 - Debian Linux 8.0 DSA-3402-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8124, CVE-2015-8125

Description

The scan detected that the host is missing the following update:
DSA-3402-1

Observation

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

http://www.debian.org/security/2015/dsa-3402

Debian 8.0
all
php-symfony-eventdispatcher_2.3.21+dfsg-4+deb8u2
php-symfony-security_2.3.21+dfsg-4+deb8u2
php-symfony-translation_2.3.21+dfsg-4+deb8u2
php-symfony-locale_2.3.21+dfsg-4+deb8u2
php-symfony-process_2.3.21+dfsg-4+deb8u2
php-symfony-event-dispatcher_2.3.21+dfsg-4+deb8u2
php-symfony-templating_2.3.21+dfsg-4+deb8u2
php-symfony-monolog-bridge_2.3.21+dfsg-4+deb8u2
php-symfony-config_2.3.21+dfsg-4+deb8u2
php-symfony-class-loader_2.3.21+dfsg-4+deb8u2
php-symfony-twig-bundle_2.3.21+dfsg-4+deb8u2
php-symfony-options-resolver_2.3.21+dfsg-4+deb8u2
php-symfony-debug_2.3.21+dfsg-4+deb8u2
php-symfony-classloader_2.3.21+dfsg-4+deb8u2
php-symfony-doctrine-bridge_2.3.21+dfsg-4+deb8u2
php-symfony-proxy-manager-bridge_2.3.21+dfsg-4+deb8u2
php-symfony-stopwatch_2.3.21+dfsg-4+deb8u2
php-symfony-propel1-bridge_2.3.21+dfsg-4+deb8u2
php-symfony-http-foundation_2.3.21+dfsg-4+deb8u2
php-symfony-filesystem_2.3.21+dfsg-4+deb8u2
php-symfony-browser-kit_2.3.21+dfsg-4+deb8u2
php-symfony-form_2.3.21+dfsg-4+deb8u2
php-symfony-console_2.3.21+dfsg-4+deb8u2
php-symfony-swiftmailer-bridge_2.3.21+dfsg-4+deb8u2
php-symfony-dom-crawler_2.3.21+dfsg-4+deb8u2
php-symfony-framework-bundle_2.3.21+dfsg-4+deb8u2
php-symfony-finder_2.3.21+dfsg-4+deb8u2
php-symfony-yaml_2.3.21+dfsg-4+deb8u2
php-symfony-css-selector_2.3.21+dfsg-4+deb8u2
php-symfony-web-profiler-bundle_2.3.21+dfsg-4+deb8u2
php-symfony-intl_2.3.21+dfsg-4+deb8u2
php-symfony-routing_2.3.21+dfsg-4+deb8u2
php-symfony-serializer_2.3.21+dfsg-4+deb8u2
php-symfony-twig-bridge_2.3.21+dfsg-4+deb8u2
php-symfony-dependency-injection_2.3.21+dfsg-4+deb8u2
php-symfony-security-bundle_2.3.21+dfsg-4+deb8u2
php-symfony-property-access_2.3.21+dfsg-4+deb8u2
php-symfony-validator_2.3.21+dfsg-4+deb8u2
php-symfony-http-kernel_2.3.21+dfsg-4+deb8u2

141005 - Red Hat Enterprise Linux RHSA-2015-2369 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3248

Description

The scan detected that the host is missing the following update:
RHSA-2015-2369

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2369.html

RHEL7D
x86_64
openhpi-devel-3.4.0-2.el7
openhpi-debuginfo-3.4.0-2.el7
openhpi-3.4.0-2.el7
openhpi-libs-3.4.0-2.el7

RHEL7WS
x86_64
openhpi-devel-3.4.0-2.el7
openhpi-debuginfo-3.4.0-2.el7
openhpi-3.4.0-2.el7
openhpi-libs-3.4.0-2.el7

141007 - Red Hat Enterprise Linux RHSA-2015-2237 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2675

Description

The scan detected that the host is missing the following update:
RHSA-2015-2237

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2237.html

RHEL7D
x86_64
rest-devel-0.7.92-3.el7
rest-debuginfo-0.7.92-3.el7
rest-0.7.92-3.el7

RHEL7WS
x86_64
rest-devel-0.7.92-3.el7
rest-debuginfo-0.7.92-3.el7
rest-0.7.92-3.el7

181686 - FreeBSD a2ps Format String Vulnerability (e359051d-90bd-11e5-bd18-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8107

Description

The scan detected that the host is missing the following update:
a2ps -- format string vulnerability (e359051d-90bd-11e5-bd18-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/e359051d-90bd-11e5-bd18-002590263bf5.html

Affected packages:
a2ps < 4.13b_8

181687 - FreeBSD kibana4 CSRF Vulnerability (fb2475c2-9125-11e5-bd18-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8131

Description

The scan detected that the host is missing the following update:
kibana4 -- CSRF vulnerability (fb2475c2-9125-11e5-bd18-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/fb2475c2-9125-11e5-bd18-002590263bf5.html

Affected packages:
4.0.0 <= kibana4 < 4.1.3
4.0.0 <= kibana41 < 4.1.3
4.2.0 <= kibana42 < 4.2.1

185062 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2816-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8213

Description

The scan detected that the host is missing the following update:
USN-2816-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003198.html

Ubuntu 12.04

python-django_1.3.1-4ubuntu1.19

Ubuntu 15.04

python3-django_1.7.6-1ubuntu2.3
python-django_1.7.6-1ubuntu2.3

Ubuntu 15.10

python-django_1.7.9-1ubuntu5.1
python3-django_1.7.9-1ubuntu5.1

Ubuntu 14.04

python-django_1.6.1-2ubuntu0.11

189998 - Fedora Linux 23 FEDORA-2015-a0ac3df0f0 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-2015-a0ac3df0f0

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172487.html

Fedora Core 23

ProDy-1.7.1-1.fc23

189999 - Fedora Linux 21 FEDORA-2015-68f5a5ba94 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-2015-68f5a5ba94

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172600.html

Fedora Core 21

ProDy-1.7.1-1.fc21

190001 - Fedora Linux 23 FEDORA-2015-0c153d3319 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-2015-0c153d3319

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172090.html

Fedora Core 23

perl-IPTables-Parse-1.5-2.fc23

190002 - Fedora Linux 23 FEDORA-2015-ca11983963 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-2015-ca11983963

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172083.html

Fedora Core 23

m2crypto-0.22.5-2.fc23

190003 - Fedora Linux 23 FEDORA-2015-f2d45d982b 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-2015-f2d45d982b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172471.html

Fedora Core 23

COPASI-4.16-0.19.20150817git3bc4e9.fc23

190004 - Fedora Linux 23 FEDORA-2015-7ebe03e30b 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-2015-7ebe03e30b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172417.html

Fedora Core 23

sundials-2.6.2-11.fc23

190006 - Fedora Linux 22 FEDORA-2015-79a3823771 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-2015-79a3823771

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172294.html

Fedora Core 22

sundials-2.6.2-11.fc22

190008 - Fedora Linux 23 FEDORA-2015-a21f0df7e5 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-2015-a21f0df7e5

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172429.html

Fedora Core 23

python-rauth-0.7.2-1.fc23

190012 - Fedora Linux 22 FEDORA-2015-12813acfa3 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-2015-12813acfa3

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172099.html

Fedora Core 22

monitorix-3.8.1-1.fc22

190014 - Fedora Linux 22 FEDORA-2015-dbc15897fb 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-2015-dbc15897fb

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172577.html

Fedora Core 22

ProDy-1.7.1-1.fc22

190022 - Fedora Linux 22 FEDORA-2015-5e566cf3e8 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-2015-5e566cf3e8

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172569.html

Fedora Core 22

COPASI-4.16-0.19.20150817git3bc4e9.fc22

190023 - Fedora Linux 22 FEDORA-2015-321ae39ee6 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-2015-321ae39ee6

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172123.html

Fedora Core 22

m2crypto-0.22.5-2.fc22

190025 - Fedora Linux 23 FEDORA-2015-d02feebd15 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5317, CVE-2015-5318, CVE-2015-5319, CVE-2015-5320, CVE-2015-5321, CVE-2015-5322, CVE-2015-5323, CVE-2015-5324, CVE-2015-5325, CVE-2015-5326

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d02feebd15

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172428.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172425.html

Fedora Core 23

jenkins-1.625.2-2.fc23
jenkins-remoting-2.53-1.fc23

190027 - Fedora Linux 22 FEDORA-2015-30f080e459 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-2015-30f080e459

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172122.html

Fedora Core 22

perl-IPTables-Parse-1.5-2.fc22

190032 - Fedora Linux 21 FEDORA-2015-240dd21cb6 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-2015-240dd21cb6

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172203.html

Fedora Core 21

perl-IPTables-Parse-1.5-2.fc21

190037 - Fedora Linux 23 FEDORA-2015-b6b8582f4e 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-2015-b6b8582f4e

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172011.html

Fedora Core 23

monitorix-3.8.1-1.fc23

190038 - Fedora Linux 21 FEDORA-2015-446074b60f 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-2015-446074b60f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172201.html

Fedora Core 21

m2crypto-0.22.5-2.fc21

190039 - Fedora Linux 21 FEDORA-2015-038912089d 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-2015-038912089d

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172318.html

Fedora Core 21

sundials-2.6.2-11.fc21

190040 - Fedora Linux 23 FEDORA-2015-c6e13cfd18 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-2015-c6e13cfd18

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172468.html

Fedora Core 23

rpm-4.13.0-0.rc1.7.fc23

190042 - Fedora Linux 21 FEDORA-2015-d292a98f01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8076

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d292a98f01

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172217.html

Fedora Core 21

cyrus-imapd-2.4.18-1.fc21

91936 - Oracle Enterprise Linux ELSA-2015-2111 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-1345

Description

The scan detected that the host is missing the following update:
ELSA-2015-2111

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005555.html

OEL7
x86_64
grep-2.20-2.el7

91937 - Oracle Enterprise Linux ELSA-2015-2401 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5281

Description

The scan detected that the host is missing the following update:
ELSA-2015-2401

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005569.html

OEL7
x86_64
grub2-efi-2.02-0.29.0.1.el7
grub2-efi-modules-2.02-0.29.0.1.el7
grub2-2.02-0.29.0.1.el7
grub2-tools-2.02-0.29.0.1.el7

91953 - Oracle Enterprise Linux ELSA-2015-2378 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3455

Description

The scan detected that the host is missing the following update:
ELSA-2015-2378

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005571.html

OEL7
x86_64
squid-sysvinit-3.3.8-26.el7
squid-3.3.8-26.el7

140994 - Red Hat Enterprise Linux RHSA-2015-2401 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5281

Description

The scan detected that the host is missing the following update:
RHSA-2015-2401

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2401.html

RHEL7D
x86_64
grub2-efi-2.02-0.29.el7
grub2-debuginfo-2.02-0.29.el7
grub2-tools-2.02-0.29.el7
grub2-efi-modules-2.02-0.29.el7
grub2-2.02-0.29.el7

RHEL7WS
x86_64
grub2-efi-2.02-0.29.el7
grub2-debuginfo-2.02-0.29.el7
grub2-tools-2.02-0.29.el7
grub2-efi-modules-2.02-0.29.el7
grub2-2.02-0.29.el7

140996 - Red Hat Enterprise Linux RHSA-2015-2378 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3455

Description

The scan detected that the host is missing the following update:
RHSA-2015-2378

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2378.html

RHEL7WS
x86_64
squid-3.3.8-26.el7
squid-debuginfo-3.3.8-26.el7
squid-sysvinit-3.3.8-26.el7

141009 - Red Hat Enterprise Linux RHSA-2015-2111 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-1345

Description

The scan detected that the host is missing the following update:
RHSA-2015-2111

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2111.html

RHEL7D
x86_64
grep-2.20-2.el7
grep-debuginfo-2.20-2.el7

RHEL7WS
x86_64
grep-2.20-2.el7
grep-debuginfo-2.20-2.el7

144054 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2032-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8025

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2032-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00102.html

SuSE Linux 13.1
x86_64
xscreensaver-debugsource-5.22-2.25.1
xscreensaver-debuginfo-5.22-2.25.1
xscreensaver-5.22-2.25.1
xscreensaver-data-debuginfo-5.22-2.25.1
xscreensaver-data-extra-5.22-2.25.1
xscreensaver-data-5.22-2.25.1
xscreensaver-data-extra-debuginfo-5.22-2.25.1

i586
xscreensaver-debugsource-5.22-2.25.1
xscreensaver-debuginfo-5.22-2.25.1
xscreensaver-5.22-2.25.1
xscreensaver-data-debuginfo-5.22-2.25.1
xscreensaver-data-extra-5.22-2.25.1
xscreensaver-data-5.22-2.25.1
xscreensaver-data-extra-debuginfo-5.22-2.25.1

SuSE Linux 13.2
x86_64
xscreensaver-data-debuginfo-5.29-2.4.3

xscreensaver-data-5.29-2.4.3
xscreensaver-data-extra-5.29-2.4.3
xscreensaver-debugsource-5.29-2.4.3
xscreensaver-5.29-2.4.3
xscreensaver-data-extra-debuginfo-5.29-2.4.3
xscreensaver-debuginfo-5.29-2.4.3

i586
xscreensaver-data-debuginfo-5.29-2.4.3
xscreensaver-data-5.29-2.4.3
xscreensaver-data-extra-5.29-2.4.3
xscreensaver-debugsource-5.29-2.4.3
xscreensaver-5.29-2.4.3
xscreensaver-data-extra-debuginfo-5.29-2.4.3
xscreensaver-debuginfo-5.29-2.4.3

144056 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2053-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8025

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2053-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001685.html

SuSE SLED 12
x86_64
xscreensaver-5.22-6.1
xscreensaver-debugsource-5.22-6.1
xscreensaver-debuginfo-5.22-6.1
xscreensaver-data-debuginfo-5.22-6.1
xscreensaver-data-5.22-6.1

SuSE SLES 12
x86_64
xscreensaver-5.22-6.1
xscreensaver-debugsource-5.22-6.1
xscreensaver-debuginfo-5.22-6.1
xscreensaver-data-debuginfo-5.22-6.1
xscreensaver-data-5.22-6.1

170587 - Amazon Linux AMI ALAS-2015-610 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7872

Description

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

ALAS-2015-610

Observation

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

https://alas.aws.amazon.com/ALAS-2015-610.html

Amazon Linux AMI
i686
kernel-devel-4.1.13-18.26.amzn1
kernel-debuginfo-common-i686-4.1.13-18.26.amzn1
perf-debuginfo-4.1.13-18.26.amzn1
kernel-tools-4.1.13-18.26.amzn1
kernel-tools-debuginfo-4.1.13-18.26.amzn1
perf-4.1.13-18.26.amzn1
kernel-debuginfo-4.1.13-18.26.amzn1
kernel-headers-4.1.13-18.26.amzn1
kernel-tools-devel-4.1.13-18.26.amzn1
kernel-4.1.13-18.26.amzn1

noarch
kernel-doc-4.1.13-18.26.amzn1

x86_64
kernel-devel-4.1.13-18.26.amzn1
perf-4.1.13-18.26.amzn1
perf-debuginfo-4.1.13-18.26.amzn1
kernel-tools-4.1.13-18.26.amzn1
kernel-tools-debuginfo-4.1.13-18.26.amzn1
kernel-debuginfo-common-x86_64-4.1.13-18.26.amzn1
kernel-debuginfo-4.1.13-18.26.amzn1
kernel-headers-4.1.13-18.26.amzn1
kernel-tools-devel-4.1.13-18.26.amzn1
kernel-4.1.13-18.26.amzn1

190021 - Fedora Linux 23 FEDORA-2015-c3b4fef3af Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5281

Description

The scan detected that the host is missing the following update:
FEDORA-2015-c3b4fef3af

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172611.html

Fedora Core 23

grub2-2.02-0.24.fc23

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.

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

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

Risk Level: High

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

Update Details

Recommendation is updated

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

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

Risk Level: High

CVE: CVE-2009-0568

Update Details

Recommendation is updated

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

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

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

Risk Level: High

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

Update Details

Recommendation is updated

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

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

Risk Level: High

CVE: CVE-2009-0568

Update Details

Recommendation is updated

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

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

8182 - Apache HTTP Server MIME Header Denial of Service Vulnerability

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

Risk Level: High

CVE: CVE-1999-0926

Update Details

FASLScript is updated

8529 - (MS10-020) Microsoft Windows SMB Client Memory Allocation Vulnerability (980232)

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

Risk Level: High

CVE: CVE-2010-0269

Update Details

Recommendation is updated

8530 - (MS10-020) Microsoft Windows SMB Client Transaction Vulnerability (980232)

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

Risk Level: High

CVE: CVE-2010-0270

Update Details

Recommendation is updated

8531 - (MS10-020) Microsoft Windows SMB Client Response Parsing Vulnerability (980232)

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

Risk Level: High

CVE: CVE-2010-0476

Update Details

Recommendation is updated

8532 - (MS10-020) Microsoft Windows SMB Client Message Size Vulnerability (980232)

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

Risk Level: High

CVE: CVE-2010-0477

Update Details

Recommendation is updated

12206 - (MS11-043) Microsoft Windows SMB Client Could Allow Remote Code Execution (KB2536276)

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

Risk Level: High

CVE: CVE-2011-1268

Update Details

Recommendation is updated

12229 - (MS11-043) Microsoft Windows SMB Client Could Allow Remote Code Execution (2536276)

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

Risk Level: High

CVE: CVE-2011-1268

Update Details

Recommendation is updated

14377 - (MS12-075) Microsoft Windows Font Parsing Remote Code Execution (2761226)

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

Risk Level: High

CVE: CVE-2012-2897

Update Details

Recommendation is updated

14381 - (MS12-075) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)

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

Risk Level: High

CVE: CVE-2012-2530, CVE-2012-2553, CVE-2012-2897

Update Details

Recommendation is updated

14495 - (MS12-078) Microsoft Windows True Type Font Parsing Remote Code Execution (2783534)

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

Risk Level: High

CVE: CVE-2012-4786

Update Details

Recommendation is updated

14501 - (MS12-078) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)

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

Risk Level: High

CVE: CVE-2012-2556, CVE-2012-4786

Update Details

Recommendation is updated

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

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: High

CVE: CVE-2013-7331

Update Details

Recommendation is updated

17223 - (MS14-057) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)

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

Risk Level: High

CVE: CVE-2014-4073, CVE-2014-4121, CVE-2014-4122

Update Details

Recommendation is updated

17225 - (MS14-057) Microsoft .NET Framework Remote Code Execution (3000414)

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

Risk Level: High

CVE: CVE-2014-4121

Update Details

Recommendation is updated

17226 - (MS14-057) Microsoft .NET Framework ClickOnce Privilege Escalation (3000414)

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

Risk Level: High

CVE: CVE-2014-4073

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

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

18878 - (MS15-093) Security Update for Internet Explorer (3088903)

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

Risk Level: High

CVE: CVE-2015-2502

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

5126 - (MS07-025) Microsoft Office Drawing Object Vulnerability (934873)

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

Risk Level: High

CVE: CVE-2007-1747

Update Details

Recommendation is updated

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

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

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

5812 - (MS08-019) Microsoft Visio Memory Validation Vulnerability (949032)

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

Risk Level: High

CVE: CVE-2008-1089, CVE-2008-1090

Update Details

Recommendation is updated

5813 - (MS08-019) Microsoft Visio Object Header Vulnerability (949032)

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

Risk Level: High

CVE: CVE-2008-1089, CVE-2008-1090

Update Details

Recommendation is updated

5862 - (MS08-026) Microsoft Object Parsing Vulnerability (951207)

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

Risk Level: High

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

Update Details

Recommendation is updated

5863 - (MS08-026) Microsoft Word Cascading Style Sheet (CSS) Vulnerability (951207)

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

Risk Level: High

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

Update Details

Recommendation is updated

5864 - (MS08-027) Microsoft Publisher Object Handler Validation Vulnerability (951208)

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

Risk Level: High

CVE: CVE-2008-0119

Update Details

Recommendation is updated

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

6064 - (MS08-051) Microsoft Memory Allocation Vulnerability (949785)

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

Risk Level: High

CVE: CVE-2008-0120 , CVE-2008-0121, CVE-2008-1455

Update Details

Recommendation is updated

6065 - (MS08-051) Microsoft Memory Calculation Vulnerability (949785)

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

Risk Level: High

CVE: CVE-2008-0120, CVE-2008-0121 , CVE-2008-1455

Update Details

Recommendation is updated

6066 - (MS08-051) Microsoft Parsing Overflow Vulnerability (949785)

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

Risk Level: High

CVE: CVE-2008-0120, CVE-2008-0121, CVE-2008-1455

Update Details

Recommendation is updated

6104 - (MS08-055) Microsoft Uniform Resource Locator Validation Error Vulnerability (955047)

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

Risk Level: High

CVE: CVE-2008-3007

Update Details

Recommendation is updated

6105 - (MS08-052) Microsoft GDI+ VML Buffer Overrun Vulnerability (954593)

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6106 - (MS08-052) Microsoft GDI+ EMF Memory Corruption Vulnerability (954593)

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6107 - (MS08-052) Microsoft GDI+ GIF Parsing Vulnerability (954593)

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6108 - (MS08-052) Microsoft GDI+WMF Buffer Overrun Vulnerability (954593)

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6109 - (MS08-052) Microsoft GDI+ BMP Integer Overflow Vulnerability (954593)

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

6220 - (MS08-068) Microsoft SMB Credential Reflection Vulnerability (957097)

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

Risk Level: High

CVE: CVE-2008-4037

Update Details

Recommendation is updated

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

6420 - (MS09-005) Microsoft Visio Memory Corruption Vulnerability - CVE-2009-0096 - (957634)

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

Risk Level: High

CVE: CVE-2009-0096

Update Details

Recommendation is updated

6421 - (MS09-005) Microsoft Visio Memory Corruption Vulnerability - CVE-2009-0097 - (957634)

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

Risk Level: High

CVE: CVE-2009-0097

Update Details

Recommendation is updated

6583 - (MS09-017) Microsoft PowerPoint Memory Corruption Vulnerability II (967340)

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

Risk Level: High

CVE: CVE-2009-0556

Update Details

Recommendation is updated

6662 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability (967340)

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

Risk Level: High

CVE: CVE-2009-0220

Update Details

Recommendation is updated

6663 - (MS09-017) Microsoft PowerPoint Integer Overflow Vulnerability (967340)

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

Risk Level: High

CVE: CVE-2009-0221

Update Details

Recommendation is updated

6664 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability II (967340)

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

Risk Level: High

CVE: CVE-2009-0222

Update Details

Recommendation is updated

6665 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability III (967340)

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

Risk Level: High

CVE: CVE-2009-0223

Update Details

Recommendation is updated

6666 - (MS09-017) Microsoft PowerPoint Memory Corruption Vulnerability (967340)

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

Risk Level: High

CVE: CVE-2009-0224

Update Details

Recommendation is updated

6667 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability IV (967340)

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

Risk Level: High

CVE: CVE-2009-0225

Update Details

Recommendation is updated

6668 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability V (967340)

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

Risk Level: High

CVE: CVE-2009-0226

Update Details

Recommendation is updated

6669 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability VI (967340)

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

Risk Level: High

CVE: CVE-2009-0227

Update Details

Recommendation is updated

6670 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability VII (967340)

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

Risk Level: High

CVE: CVE-2009-1128

Update Details

Recommendation is updated

6671 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability VIII (967340)

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

Risk Level: High

CVE: CVE-2009-1129

Update Details

Recommendation is updated

6672 - (MS09-017) Microsoft PowerPoint Heap Corruption Vulnerability (967340)

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

Risk Level: High

CVE: CVE-2009-1130

Update Details

Recommendation is updated

6673 - (MS09-017) Microsoft PowerPoint Legacy File Format Vulnerability IX (967340)

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

Risk Level: High

CVE: CVE-2009-1137

Update Details

Recommendation is updated

6674 - (MS09-017) Microsoft PowerPoint Data Out of Bounds Vulnerability (967340)

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

Risk Level: High

CVE: CVE-2009-1131

Update Details

Recommendation is updated

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

6841 - (MS09-030) Microsoft Publisher Pointer Dereference Vulnerability (969516)

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

Risk Level: High

CVE: CVE-2009-0566

Update Details

Recommendation is updated

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

7318 - (MS09-065) Win32k EOT Parsing Vulnerability (969947)

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

Risk Level: High

CVE: CVE-2009-2514

Update Details

Recommendation is updated

7319 - (MS09-067) Excel Cache Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3127

Update Details

Recommendation is updated

7320 - (MS09-067) Excel SxView Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3128

Update Details

Recommendation is updated

7321 - (MS09-067) Excel Featheader Record Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3129

Update Details

Recommendation is updated

7322 - (MS09-067) Excel Document Parsing Heap Overflow Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3130

Update Details

Recommendation is updated

7323 - (MS09-067) Excel Formula Parsing Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3131

Update Details

Recommendation is updated

7324 - (MS09-067) Excel Index Parsing Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3132

Update Details

Recommendation is updated

7325 - (MS09-067) Excel Document Parsing Memory Corruption Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3133

Update Details

Recommendation is updated

7326 - (MS09-067) Excel Field Sanitization Vulnerability (972652)

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

Risk Level: High

CVE: CVE-2009-3134

Update Details

Recommendation is updated

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

7356 - (MS09-017) Vulnerabilities In Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)

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

Risk Level: High

CVE: CVE-2009-0220, CVE-2009-0221, CVE-2009-0222, CVE-2009-0223, CVE-2009-0224, CVE-2009-0225, CVE-2009-0226, CVE-2009-0227, CVE-2009-0556, CVE-2009-1128, CVE-2009-1129, CVE-2009-1130, CVE-2009-1131, CVE-2009-1137

Update Details

Recommendation is updated

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

7412 - (MS09-005) Vulnerabilities In Microsoft Office Visio Could Allow Remote Code Execution (957634)

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

Risk Level: High

CVE: CVE-2009-0095, CVE-2009-0096, CVE-2009-0097

Update Details

Recommendation is updated

7413 - (MS09-006) Vulnerabilities In Windows Kernel Could Allow Remote Code Execution (958690)

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

Risk Level: High

CVE: CVE-2009-0081, CVE-2009-0082, CVE-2009-0083

Update Details

Recommendation is updated

7416 - (MS09-009) Vulnerabilities In Microsoft Office Excel Could Cause Remote Code Execution (968557)

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

Risk Level: High

CVE: CVE-2009-0100, CVE-2009-0238

Update Details

Recommendation is updated

7549 - (MS09-030) Vulnerability In Microsoft Office Publisher Could Allow Remote Code Execution (969516)

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

Risk Level: High

CVE: CVE-2009-0566

Update Details

Recommendation is updated

7639 - (MS08-051) Vulnerabilities In Microsoft PowerPoint Could Allow Remote Code Execution (949785)

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

Risk Level: High

CVE: CVE-2008-0120, CVE-2008-0121, CVE-2008-1455

Update Details

Recommendation is updated

7701 - (MS08-052) Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

7772 - (MS08-027) Vulnerability In Microsoft Publisher Could Allow Remote Code Execution (951208)

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

Risk Level: High

CVE: CVE-2008-0119

Update Details

Recommendation is updated

7809 - (MS08-055) Vulnerability in Microsoft Office Could Allow Remote Code Execution (955047)

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

Risk Level: High

CVE: CVE-2008-3007

Update Details

Recommendation is updated

7822 - (MS08-009) Vulnerability In Microsoft Word Could Allow Remote Code Execution (947077)

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

Risk Level: High

CVE: CVE-2008-0109

Update Details

Recommendation is updated

7857 - (MS10-006) Microsoft Windows SMB Client Pool Corruption Vulnerability (978251)

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

Risk Level: High

CVE: CVE-2010-0016

Update Details

Recommendation is updated

7858 - (MS10-006) Microsoft Windows SMB Client Race Condition Vulnerability (978251)

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

Risk Level: High

CVE: CVE-2010-0017

Update Details

Recommendation is updated

7880 - (MS10-006) Vulnerabilities In SMB Client Could Allow Remote Code Execution (978251)

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

Risk Level: High

CVE: CVE-2010-0016, CVE-2010-0017

Update Details

Recommendation is updated

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

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

8154 - (MS08-068) Vulnerability In SMB Could Allow Remote Code Execution (957097)

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

Risk Level: High

CVE: CVE-2008-4037

Update Details

Recommendation is updated

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

8541 - (MS10-020) Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)

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

Risk Level: High

CVE: CVE-2009-3676, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477

Update Details

Recommendation is updated

8546 - (MS10-022) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)

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

Risk Level: High

CVE: CVE-2010-0483

Update Details

Recommendation is updated

8549 - (MS10-028) Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (980094)

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

Risk Level: High

CVE: CVE-2010-0254, CVE-2010-0256

Update Details

Recommendation is updated

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

9417 - (MS10-044) Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1881, CVE-2010-0814

Update Details

Recommendation is updated

9419 - (MS10-044) Microsoft Office Access ActiveX Control Vulnerability (982335)

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

Risk Level: High

CVE: CVE-2010-0814

Update Details

Recommendation is updated

9421 - (MS10-044) Microsoft Office ACCWIZ.dll Uninitialized Variable Vulnerability (982335)

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

Risk Level: High

CVE: CVE-2010-1881

Update Details

Recommendation is updated

9681 - (MS10-049) Microsoft Windows SChannel Malformed Certificate Request Remote Code Execution (980436)

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

Risk Level: High

CVE: CVE-2010-2566

Update Details

Recommendation is updated

9707 - (MS10-056) Microsoft Office Word HTML Linked Objects Memory Corruption Vulnerability (2269638)

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

Risk Level: High

CVE: CVE-2010-1903

Update Details

Recommendation is updated

9708 - (MS10-056) Microsoft Office Word RTF Parsing Buffer Overflow Vulnerability (2269638)

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

Risk Level: High

CVE: CVE-2010-1902

Update Details

Recommendation is updated

9709 - (MS10-056) Microsoft Office Word RTF Parsing Engine Memory Corruption Vulnerability (2269638)

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

Risk Level: High

CVE: CVE-2010-1901

Update Details

Recommendation is updated

9710 - (MS10-056) Microsoft Office Word Record Parsing Vulnerability (2269638)

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

Risk Level: High

CVE: CVE-2010-1900

Update Details

Recommendation is updated

9713 - (MS10-049) Vulnerabilities in SChannel could allow Remote Code Execution (980436)

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

Risk Level: High

CVE: CVE-2009-3555, CVE-2010-2566

Update Details

Recommendation is updated

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

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

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

10653 - (MS10-087) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2423930)

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

Risk Level: High

CVE: CVE-2010-3333, CVE-2010-3334, CVE-2010-3335, CVE-2010-3336, CVE-2010-3337

Update Details

Recommendation is updated

10865 - (MS10-103) Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)

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

Risk Level: High

CVE: CVE-2010-2569, CVE-2010-2570, CVE-2010-2571 , CVE-2010-3954, CVE-2010-3955

Update Details

Recommendation is updated

10879 - (MS10-103) Microsoft Office Suites and Components Size Value Heap Corruption in pubconv.dll Vulnerability (2292970)

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

Risk Level: High

CVE: CVE-2010-2569

Update Details

Recommendation is updated

10880 - (MS10-103) Microsoft Office Suites Heap Overrun in pubconv.dll Vulnerability (2292970)

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

Risk Level: High

CVE: CVE-2010-2570

Update Details

Recommendation is updated

10881 - (MS10-103) Microsoft Office Suites Memory Corruption Due To Invalid Index Into Array in Pubconv.dll Vulnerability (2292970)

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

Risk Level: High

CVE: CVE-2010-2571

Update Details

Recommendation is updated

10882 - (MS10-103) Microsoft Publisher Memory Corruption Vulnerability (2292970)

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

Risk Level: High

CVE: CVE-2010-3954

Update Details

Recommendation is updated

10883 - (MS10-103) Microsoft Office Suites Array Indexing Memory Corruption Vulnerability (2292970)

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

Risk Level: High

CVE: CVE-2010-3955

Update Details

Recommendation is updated

11066 - (MS10-036) Microsoft Office COM Object Validation Vulnerability (983235)

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

Risk Level: High

CVE: CVE-2010-1263

Update Details

Recommendation is updated

11238 - (MS11-008) Microsoft Visio Object Memory Corruption (2451879)

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

Risk Level: High

CVE: CVE-2011-0092

Update Details

Recommendation is updated

11239 - (MS11-008) Microsoft Visio Data Type Memory Corruption (2451879)

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

Risk Level: High

CVE: CVE-2011-0093

Update Details

Recommendation is updated

11254 - (MS11-008) Vulnerabilities In Microsoft Visio Could Allow Remote Code Execution (2451879)

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

Risk Level: High

CVE: CVE-2011-0092, CVE-2011-0093

Update Details

Recommendation is updated

11340 - (MS11-022) Microsoft PowerPoint OfficeArt Atom RCE (2489283)

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

Risk Level: High

CVE: CVE-2011-0976

Update Details

Recommendation is updated

11341 - (MS11-023) Microsoft Office Graphic Object Dereferencing (2489293)

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

Risk Level: High

CVE: CVE-2011-0977

Update Details

Recommendation is updated

11342 - (MS11-021) Microsoft Excel Array Indexing (2489279)

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

Risk Level: High

CVE: CVE-2011-0978

Update Details

Recommendation is updated

11343 - (MS11-021) Microsoft Excel Linked List Corruption (2489279)

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

Risk Level: High

CVE: CVE-2011-0979

Update Details

Recommendation is updated

11344 - (MS11-021) Microsoft Excel Dangling Pointer (2489279)

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

Risk Level: High

CVE: CVE-2011-0980

Update Details

Recommendation is updated

11757 - (MS11-021) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279)

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

Risk Level: High

CVE: CVE-2011-0097, CVE-2011-0098, CVE-2011-0101, CVE-2011-0103, CVE-2011-0104, CVE-2011-0105, CVE-2011-0978, CVE-2011-0979, CVE-2011-0980

Update Details

Recommendation is updated

11758 - (MS11-022) Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2489283)

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

Risk Level: High

CVE: CVE-2011-0655, CVE-2011-0656, CVE-2011-0976

Update Details

Recommendation is updated

11759 - (MS11-023) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2489293)

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

Risk Level: High

CVE: CVE-2011-0107, CVE-2011-0977

Update Details

Recommendation is updated

11765 - (MS11-029) Vulnerability in GDI+ Could Allow Remote Code Execution (2489979)

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

Risk Level: High

CVE: CVE-2011-0041

Update Details

Recommendation is updated

11775 - (MS11-021) Microsoft Excel Integer Overrun (2489279)

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

Risk Level: High

CVE: CVE-2011-0097

Update Details

Recommendation is updated

11777 - (MS11-021) Microsoft Excel Record Parsing WriteAV (2489279)

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

Risk Level: High

CVE: CVE-2011-0101

Update Details

Recommendation is updated

11778 - (MS11-021) Microsoft Excel Memory Corruption (2489279)

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

Risk Level: High

CVE: CVE-2011-0103

Update Details

Recommendation is updated

11779 - (MS11-021) Microsoft Excel Heap Overflow (2489279)

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

Risk Level: High

CVE: CVE-2011-0098

Update Details

Recommendation is updated

11780 - (MS11-021) Microsoft Excel Buffer Overwrite (2489279)

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

Risk Level: High

CVE: CVE-2011-0104

Update Details

Recommendation is updated

11781 - (MS11-021) Microsoft Excel Data Initialization (2489279)

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

Risk Level: High

CVE: CVE-2011-0105

Update Details

Recommendation is updated

11782 - (MS11-022) Microsoft PowerPoint Floating Point Techno-color Time Bandit RCE (2489283)

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

Risk Level: High

CVE: CVE-2011-0655

Update Details

Recommendation is updated

11783 - (MS11-022) Microsoft PowerPoint Persist Directory RCE (2489283)

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

Risk Level: High

CVE: CVE-2011-0656

Update Details

Recommendation is updated

11784 - (MS11-023) Microsoft Office Component Insecure Library Loading (2489293)

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

Risk Level: High

CVE: CVE-2011-0107

Update Details

Recommendation is updated

11785 - (MS11-029) Microsoft GDI+ Integer Overflow (2489979)

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

Risk Level: High

CVE: CVE-2011-0041

Update Details

Recommendation is updated

11993 - (MS11-036) Microsoft PowerPoint Buffer Overrun RCE (2545814)

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

Risk Level: High

CVE: CVE-2011-1270

Update Details

Recommendation is updated

11994 - (MS11-036) Microsoft PowerPoint Memory Corruption RCE (2545814)

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

Risk Level: High

CVE: CVE-2011-1269

Update Details

Recommendation is updated

11996 - (MS11-036) Vulnerabilities In Microsoft PowerPoint Could Allow Remote Code Execution (2545814)

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

Risk Level: High

CVE: CVE-2011-1269, CVE-2011-1270

Update Details

Recommendation is updated

12208 - (MS11-045) Microsoft Excel Buffer Overrun Remote Code Execution (2537146)

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

Risk Level: High

CVE: CVE-2011-1276

Update Details

Recommendation is updated

12209 - (MS11-045) Microsoft Excel Improper Record Parsing Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1273

Update Details

Recommendation is updated

12210 - (MS11-045) Microsoft Excel Insufficient Record Validation Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1272

Update Details

Recommendation is updated

12213 - (MS11-045) Microsoft Excel Memory Heap Overwrite Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1275

Update Details

Recommendation is updated

12214 - (MS11-045) Microsoft Excel Out of Bounds Array Access Remote Code Execution (KB2537146)

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

Risk Level: High

CVE: CVE-2011-1274

Update Details

Recommendation is updated

12219 - (MS11-041) Microsoft Windows Kernel-Mode Drivers Could Allow Remote Code Execution (KB2525694)

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

Risk Level: High

CVE: CVE-2011-1873

Update Details

Recommendation is updated

12247 - (MS11-041) Vulnerability In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)

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

Risk Level: High

CVE: CVE-2011-1873

Update Details

Recommendation is updated

12253 - (MS11-045) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2537146)

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

Risk Level: High

CVE: CVE-2011-1272, CVE-2011-1273, CVE-2011-1274, CVE-2011-1275, CVE-2011-1276, CVE-2011-1277, CVE-2011-1278, CVE-2011-1279

Update Details

Recommendation is updated

12459 - (MS11-060) Microsoft Visio Move Around The Block Could Allow Remote Code Execution (2560978)

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

Risk Level: High

CVE: CVE-2011-1979

Update Details

Recommendation is updated

12462 - (MS11-060) Microsoft Visio Pstream Release Could Allow Remote Code Execution (2560978)

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

Risk Level: High

CVE: CVE-2011-1972

Update Details

Recommendation is updated

12469 - (MS11-060) Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2560978)

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

Risk Level: High

CVE: CVE-2011-1971, CVE-2011-1972

Update Details

Recommendation is updated

12616 - (MS11-072) Microsoft Excel Conditional Expression Parsing Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1989

Update Details

Recommendation is updated

12617 - (MS11-072) Microsoft Excel Heap Corruption Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1988

Update Details

Recommendation is updated

12618 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1987

Update Details

Recommendation is updated

12619 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution II (2587505)

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

Risk Level: High

CVE: CVE-2011-1990

Update Details

Recommendation is updated

12620 - (MS11-072) Microsoft Excel Use after Free WriteAV Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1986

Update Details

Recommendation is updated

12621 - (MS11-073) Microsoft Office Component Insecure Library Loading Remote Code Execution (2587634)

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

Risk Level: High

CVE: CVE-2011-1980

Update Details

Recommendation is updated

12622 - (MS11-073) Microsoft Office Uninitialized Object Pointer Remote Code Execution (2587634)

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

Risk Level: High

CVE: CVE-2011-1982

Update Details

Recommendation is updated

12626 - (MS11-073) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2587634)

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

Risk Level: High

CVE: CVE-2011-1980, CVE-2011-1982

Update Details

Recommendation is updated

12627 - (MS11-072) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1986, CVE-2011-1987, CVE-2011-1988, CVE-2011-1989, CVE-2011-1990

Update Details

Recommendation is updated

12740 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Font Library File Buffer Overrun (2567053)

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

Risk Level: High

CVE: CVE-2011-2003

Update Details

Recommendation is updated

12744 - (MS11-077) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)

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

Risk Level: High

CVE: CVE-2011-1985, CVE-2011-2002, CVE-2011-2003, CVE-2011-2011

Update Details

Recommendation is updated

12832 - (MS11-091) Microsoft Publisher Function Pointer Overwrite (2607702)

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

Risk Level: High

CVE: CVE-2011-1508

Update Details

Recommendation is updated

12891 - (MS11-087) Microsoft Windows TrueType Font Parsing (2639417)

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

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

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

13068 - (MS11-091) Microsoft Publisher Invalid Pointer (2607702)

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

Risk Level: High

CVE: CVE-2011-3411

Update Details

Recommendation is updated

13069 - (MS11-091) Microsoft Publisher Memory Corruption (2607702)

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

Risk Level: High

CVE: CVE-2011-3412

Update Details

Recommendation is updated

13071 - (MS11-091) Microsoft Publisher Out-of-bounds Array Index (2607702)

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

Risk Level: High

CVE: CVE-2011-3410

Update Details

Recommendation is updated

13072 - (MS11-087) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)

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

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

13076 - (MS11-091) Vulnerabilities in Microsoft Publisher Could Allow Elevation of Privilege (2607702)

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

Risk Level: High

CVE: CVE-2011-1508, CVE-2011-3410, CVE-2011-3411, CVE-2011-3412

Update Details

Recommendation is updated

13080 - (MS11-094) Microsoft PowerPoint Insecure Library Loading (2639142)

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

Risk Level: High

CVE: CVE-2011-3396

Update Details

Recommendation is updated

13081 - (MS11-094) Microsoft PowerPoint OfficeArt Shape RCE (2639142)

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

Risk Level: High

CVE: CVE-2011-3413

Update Details

Recommendation is updated

13121 - (MS12-008) Microsoft Windows GDI Access Violation (2660465)

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

Risk Level: High

CVE: CVE-2011-5046

Update Details

Recommendation is updated

13161 - (MS11-100) Microsoft .NET User Authentication Privilege Escalation (2638420)

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

Risk Level: High

CVE: CVE-2011-3416

Update Details

Recommendation is updated

13162 - (MS11-100) Microsoft .NET Cached Content Privilege Escalation (2638420)

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

Risk Level: High

CVE: CVE-2011-3417

Update Details

Recommendation is updated

13163 - (MS11-100) Vulnerabilities In .NET Framework Could Allow Elevation of Privilege (2638420)

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

Risk Level: High

CVE: CVE-2011-3414, CVE-2011-3415, CVE-2011-3416, CVE-2011-3417

Update Details

Recommendation is updated

13188 - (MS12-001) Microsoft Windows Kernel SafeSEH Bypass (2644615)

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

Risk Level: High

CVE: CVE-2012-0001

Update Details

Recommendation is updated

13191 - (MS12-001) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)

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

Risk Level: High

CVE: CVE-2012-0001

Update Details

Recommendation is updated

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

13622 - (MS12-034) Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)

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

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

Update Details

Recommendation is updated

13624 - (MS12-034) Microsoft Silverlight Double Free Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0176

Update Details

Recommendation is updated

13625 - (MS12-034) Microsoft Windows .NET Buffer Allocation Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0162

Update Details

Recommendation is updated

13629 - (MS12-034) Microsoft Windows GDI+ Heap Overflow Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0167

Update Details

Recommendation is updated

13630 - (MS12-034) Microsoft Windows GDI+ Record Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0165

Update Details

Recommendation is updated

13631 - (MS12-034) Microsoft Windows TrueType Font Parsing II (2681578)

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

Risk Level: High

CVE: CVE-2012-0159

Update Details

Recommendation is updated

13632 - (MS12-034) Microsoft Windows TrueType Font Parsing (2681578)

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

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

13782 - (MS12-039) Microsoft Lync Insecure Library Loading Remote Code Execution (2707956)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1849

Update Details

Recommendation is updated

13784 - (MS12-039) Microsoft Windows TrueType Font Parsing II Remote Code Execution (2707956)

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

Risk Level: High

CVE: CVE-2012-0159

Update Details

Recommendation is updated

13786 - (MS12-039) Microsoft Windows TrueType Font Parsing Remote Code Execution (2707956)

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

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

13788 - (MS12-039) Vulnerabilities in Lync Could Allow Remote Code Execution (2707956)

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

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-1849, CVE-2012-1858

Update Details

Recommendation is updated

14014 - (MS12-055) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)

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

Risk Level: High

CVE: CVE-2012-2527

Update Details

Recommendation is updated

14018 - (MS12-059) Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2733918)

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

Risk Level: High

CVE: CVE-2012-1888

Update Details

Recommendation is updated

14020 - (MS12-059) Microsoft Visio DXF File Format Remote Code Execution (2733918)

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

Risk Level: High

CVE: CVE-2012-1888

Update Details

Recommendation is updated

14044 - (MS12-057) Microsoft Office CGM File Format Remote Code Execution (2731879)

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

Risk Level: High

CVE: CVE-2012-2524

Update Details

Recommendation is updated

14045 - (MS12-057) Vulnerability in Microsoft Office Could Allow for Remote Code Execution (2731879)

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

Risk Level: High

CVE: CVE-2012-2524

Update Details

Recommendation is updated

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 Exeuction (2720184)

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

Risk Level: High

CVE: CVE-2012-1886

Update Details

Recommendation is updated

14357 - (MS12-076) Microsoft Excel SST Invalid Length Remote Code Execution (2720184)

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

Risk Level: High

CVE: CVE-2012-1887

Update Details

Recommendation is updated

14358 - (MS12-076) Microsoft Excel Stack Overflow Remote Code Execution (2720184)

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

Risk Level: High

CVE: CVE-2012-2543

Update Details

Recommendation is updated

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

14494 - (MS12-078) Microsoft Windows Open Type Font Parsing Remote Code Execution (2783534)

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

Risk Level: High

CVE: CVE-2012-2556

Update Details

Recommendation is updated

14648 - (MS13-019) Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)

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

Risk Level: High

CVE: CVE-2013-0076

Update Details

Recommendation is updated

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

14695 - (MS13-009) Microsoft Internet Explorer CDispNode Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0023

Update Details

Recommendation is updated

14696 - (MS13-009) Microsoft Internet Explorer CHTML Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0029

Update Details

Recommendation is updated

14697 - (MS13-009) Microsoft Internet Explorer CMarkup Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0020

Update Details

Recommendation is updated

14698 - (MS13-009) Microsoft Internet Explorer CObjectElement Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0028

Update Details

Recommendation is updated

14699 - (MS13-009) Microsoft Internet Explorer COmWindowProxy Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0019

Update Details

Recommendation is updated

14700 - (MS13-009) Microsoft Internet Explorer CPasteCommand Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0027

Update Details

Recommendation is updated

14701 - (MS13-009) Microsoft Internet Explorer InsertElement Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0026

Update Details

Recommendation is updated

14702 - (MS13-009) Microsoft Internet Explorer LsGetTrailInfo Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0022

Update Details

Recommendation is updated

14703 - (MS13-009) Microsoft Internet Explorer PasteHTML Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0024

Update Details

Recommendation is updated

14704 - (MS13-009) Microsoft Internet Explorer SetCapture Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0018

Update Details

Recommendation is updated

14706 - (MS13-009) Microsoft Internet Explorer SLayoutRun Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0025

Update Details

Recommendation is updated

14707 - (MS13-009) Microsoft Internet Explorer Vtable Use-After-Free Remote Code Execution (2792100)

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

Risk Level: High

CVE: CVE-2013-0021

Update Details

Recommendation is updated

14719 - (MS13-017) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)

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

Risk Level: High

CVE: CVE-2013-1278, CVE-2013-1279, CVE-2013-1280

Update Details

Recommendation is updated

14928 - (MS13-036) Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege (2829996)

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

Risk Level: High

CVE: CVE-2013-1283, CVE-2013-1291, CVE-2013-1292, CVE-2013-1293

Update Details

Recommendation is updated

15052 - (MS13-041) Vulnerability in Lync Could Allow Remote Code Execution (2834695)

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

Risk Level: High

CVE: CVE-2013-1302

Update Details

Recommendation is updated

15053 - (MS13-041) Microsoft Office Lync Remote Code Execution (2834695)

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

Risk Level: High

CVE: CVE-2013-1302

Update Details

Recommendation is updated

15057 - (MS13-042) Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1316, CVE-2013-1317, CVE-2013-1318, CVE-2013-1319, CVE-2013-1320, CVE-2013-1321, CVE-2013-1322, CVE-2013-1323, CVE-2013-1327, CVE-2013-1328, CVE-2013-1329

Update Details

Recommendation is updated

15058 - (MS13-042) Microsoft Office Publisher Negative Value Allocation Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1316

Update Details

Recommendation is updated

15059 - (MS13-042) Microsoft Office Publisher Integer Overflow Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1317

Update Details

Recommendation is updated

15060 - (MS13-042) Microsoft Office Publisher Corrupt Interface Pointer Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1318

Update Details

Recommendation is updated

15061 - (MS13-042) Microsoft Office Publisher Return Value Handling Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1319

Update Details

Recommendation is updated

15062 - (MS13-042) Microsoft Office Publisher Return Value Validation Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1321

Update Details

Recommendation is updated

15063 - (MS13-042) Microsoft Office Publisher Buffer Overflow Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1320

Update Details

Recommendation is updated

15064 - (MS13-042) Microsoft Office Publisher Invalid Range Check Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1322

Update Details

Recommendation is updated

15065 - (MS13-042) Microsoft Office Publisher Incorrect NULL Value Handling Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1323

Update Details

Recommendation is updated

15066 - (MS13-042) Microsoft Office Publisher Signed Integer Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1327

Update Details

Recommendation is updated

15067 - (MS13-042) Microsoft Office Publisher Pointer Handling Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1328

Update Details

Recommendation is updated

15068 - (MS13-042) Microsoft Office Publisher Buffer Underflow Remote Code Execution (2830397)

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

Risk Level: High

CVE: CVE-2013-1329

Update Details

Recommendation is updated

15242 - (MS13-053) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-1300, CVE-2013-1340, CVE-2013-1345, CVE-2013-3129, CVE-2013-3167, CVE-2013-3172, CVE-2013-3173, CVE-2013-3660

Update Details

Recommendation is updated

15256 - (MS13-054) Microsoft Windows TrueType Font Parsing Remote Code Execution (2848295)

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

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15258 - (MS13-053) Microsoft Windows Kernel Buffer Overwrite Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-3173

Update Details

Recommendation is updated

15259 - (MS13-053) Microsoft Windows Kernel Dereference Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-1340

Update Details

Recommendation is updated

15261 - (MS13-054) Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)

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

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15280 - (MS13-053) Microsoft Windows Kernel Memory Allocation Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-1300

Update Details

Recommendation is updated

15282 - (MS13-053) Microsoft Windows Kernel Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-1345

Update Details

Recommendation is updated

15283 - (MS13-053) Microsoft Windows Kernel TrueType Font Parsing Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15284 - (MS13-053) Microsoft Windows Win32k Information Disclosure (2850851)

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

Risk Level: High

CVE: CVE-2013-3167

Update Details

Recommendation is updated

15387 - (MS13-062) Microsoft Windows Remote Procedure Call Privilege Escalation (2849470)

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

Risk Level: High

CVE: CVE-2013-3175

Update Details

Recommendation is updated

15388 - (MS13-062) Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)

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

Risk Level: High

CVE: CVE-2013-3175

Update Details

Recommendation is updated

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

15734 - (MS13-081) Microsoft Windows TrueType Font CMAP Remote Code Execution (2870008)

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

Risk Level: High

CVE: CVE-2013-3894

Update Details

Recommendation is updated

15740 - (MS13-081) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)

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

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3200, CVE-2013-3879, CVE-2013-3880, CVE-2013-3881, CVE-2013-3888, CVE-2013-3894

Update Details

Recommendation is updated

15751 - (MS13-081) Microsoft Windows Kernel-Mode Driver OpenType Font Parsing Remote Code Execution (2870008)

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

Risk Level: High

CVE: CVE-2013-3128

Update Details

Recommendation is updated

15928 - (MS13-088) Cumulative Security Update for Internet Explorer (2888505)

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

Risk Level: High

CVE: CVE-2013-3871, CVE-2013-3908, CVE-2013-3909, CVE-2013-3910, CVE-2013-3911, CVE-2013-3912, CVE-2013-3914, CVE-2013-3915, CVE-2013-3916, CVE-2013-3917

Update Details

Recommendation is updated

15932 - (MS13-091) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)

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

Risk Level: High

CVE: CVE-2013-0082, CVE-2013-1324, CVE-2013-1325

Update Details

Recommendation is updated

16013 - (MS13-096) Vulnerability In Microsoft Graphics Component Could Allow Remote Code Execution (2908005)

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

Risk Level: High

CVE: CVE-2013-3906

Update Details

Recommendation is updated

16019 - (MS13-097) Cumulative Security Update for Internet Explorer (2898785)

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

Risk Level: High

CVE: CVE-2013-5045, CVE-2013-5046, CVE-2013-5047, CVE-2013-5048, CVE-2013-5049, CVE-2013-5051, CVE-2013-5052

Update Details

Recommendation is updated

16020 - (MS13-097) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2898785)

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

Risk Level: High

CVE: CVE-2013-5052

Update Details

Recommendation is updated

16026 - (MS13-097) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2898785)

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

Risk Level: High

CVE: CVE-2013-5051

Update Details

Recommendation is updated

16027 - (MS13-097) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2898785)

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

Risk Level: High

CVE: CVE-2013-5049

Update Details

Recommendation is updated

16028 - (MS13-097) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2898785)

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

Risk Level: High

CVE: CVE-2013-5048

Update Details

Recommendation is updated

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

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

16366 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0281

Update Details

Recommendation is updated

16405 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0324

Update Details

Recommendation is updated

16406 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0322

Update Details

Recommendation is updated

16407 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0321

Update Details

Recommendation is updated

16408 - (MS14-012) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0314

Update Details

Recommendation is updated

16409 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0313

Update Details

Recommendation is updated

16410 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0312

Update Details

Recommendation is updated

16411 - (MS14-012) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0311

Update Details

Recommendation is updated

16412 - (MS14-012) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0309

Update Details

Recommendation is updated

16413 - (MS14-012) Microsoft Internet Explorer Memory Corruption X Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0308

Update Details

Recommendation is updated

16414 - (MS14-012) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0307

Update Details

Recommendation is updated

16415 - (MS14-012) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0306

Update Details

Recommendation is updated

16416 - (MS14-012) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0305

Update Details

Recommendation is updated

16417 - (MS14-012) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0304

Update Details

Recommendation is updated

16418 - (MS14-012) Microsoft Internet Explorer Memory Corruption V Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0303

Update Details

Recommendation is updated

16419 - (MS14-012) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0302

Update Details

Recommendation is updated

16420 - (MS14-012) Microsoft Internet Explorer Memory Corruption III Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0299

Update Details

Recommendation is updated

16421 - (MS14-012) Microsoft Internet Explorer Memory Corruption II Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0298

Update Details

Recommendation is updated

16422 - (MS14-012) Microsoft Internet Explorer Memory Corruption I Remote Code Execution(2925418)

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

Risk Level: High

CVE: CVE-2014-0297

Update Details

Recommendation is updated

16423 - (MS14-012) Cumulative Security Update for Internet Explorer (2925418)

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

Risk Level: High

CVE: CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, CVE-2014-0322, CVE-2014-0324

Update Details

Recommendation is updated

16483 - (MS14-018) Cumulative Security Update for Internet Explorer (2950467)

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

Risk Level: High

CVE: CVE-2014-0325, 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-2014-0325, CVE-2014-3538

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

16490 - (MS14-020) Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (2950145)

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

Risk Level: High

CVE: CVE-2014-1759

Update Details

Recommendation is updated

16492 - (MS14-017) Vulnerabilities In Microsoft Word And Office Web Apps Could Allow Remote Code Execution (2949660)

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

Risk Level: High

CVE: CVE-2014-1757, CVE-2014-1758, CVE-2014-1761

Update Details

Recommendation is updated

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

16839 - (MS14-038) Vulnerability In Windows Journal Could Allow Remote Code Execution (2975689)

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

Risk Level: High

CVE: CVE-2014-1824

Update Details

Recommendation is updated

16844 - (MS14-038) Microsoft Windows Journal Remote Code Execution (2975689)

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

Risk Level: High

CVE: CVE-2014-1824

Update Details

Recommendation is updated

16847 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2802

Update Details

Recommendation is updated

16848 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2801

Update Details

Recommendation is updated

16849 - (MS14-037) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2975687)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2800

Update Details

Recommendation is updated

16850 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2798

Update Details

Recommendation is updated

16851 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2797

Update Details

Recommendation is updated

16852 - (MS14-037) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2795

Update Details

Recommendation is updated

16853 - (MS14-037) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2794

Update Details

Recommendation is updated

16854 - (MS14-037) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2792

Update Details

Recommendation is updated

16855 - (MS14-037) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2791

Update Details

Recommendation is updated

16856 - (MS14-037) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2790

Update Details

Recommendation is updated

16857 - (MS14-037) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2789

Update Details

Recommendation is updated

16858 - (MS14-037) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2788

Update Details

Recommendation is updated

16859 - (MS14-037) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2787

Update Details

Recommendation is updated

16860 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2804

Update Details

Recommendation is updated

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

17002 - (MS14-048) Microsoft OneNote File Parsing Remote Code Execution (2977201)

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

Risk Level: High

CVE: CVE-2014-2815

Update Details

Recommendation is updated

17009 - (MS14-048) Vulnerability in OneNote Could Allow Remote Code Execution (2977201)

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

Risk Level: High

CVE: CVE-2014-2815

Update Details

Recommendation is updated

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

17101 - (MS14-052) Cumulative Security Update for Internet Explorer (2977629)

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

Risk Level: High

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

17227 - (MS14-058) Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)

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

Risk Level: High

CVE: CVE-2014-4113, CVE-2014-4148

Update Details

Recommendation is updated

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

17250 - (MS14-058) Microsoft Windows TrueType Font Parsing Remote Code Execution (3000061)

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

Risk Level: High

CVE: CVE-2014-4148

Update Details

Recommendation is updated

17257 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

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

Risk Level: High

CVE: CVE-2014-4117

Update Details

Recommendation is updated

17258 - (MS14-061) Microsoft Word File Format Remote Code Execution (3000434)

Category: Windows Host Assessment -> Patches and Hotfixes
(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

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

17386 - (MS14-069) Microsoft Word Invalid Pointer Remote Code Execution (3009710)

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

Risk Level: High

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: High

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: High

CVE: CVE-2014-6333

Update Details

Recommendation is updated

17397 - (MS14-078) Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)

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

Risk Level: High

CVE: CVE-2014-4077

Update Details

Recommendation is updated

17398 - (MS14-078) Microsoft Windows IME (Japanese) Privilege Escalation (2992719)

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

Risk Level: High

CVE: CVE-2014-4077

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

17485 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (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

17486 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (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

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

17490 - (MS14-083) Microsoft Excel Global Free Remote Code Execution (3017347)

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

Risk Level: High

CVE: CVE-2014-6360

Update Details

Recommendation is updated

17491 - (MS14-083) Microsoft Excel Excel Invalid Pointer Remote Code Execution (3017347)

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

Risk Level: High

CVE: CVE-2014-6361

Update Details

Recommendation 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

17795 - (MS15-009) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0017

Update Details

Recommendation is updated

17796 - (MS15-009) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0018

Update Details

Recommendation is updated

17797 - (MS15-009) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0019

Update Details

Recommendation is updated

17798 - (MS15-009) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0020

Update Details

Recommendation is updated

17799 - (MS15-009) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0021

Update Details

Recommendation is updated

17800 - (MS15-009) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0022

Update Details

Recommendation is updated

17801 - (MS15-009) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0023

Update Details

Recommendation is updated

17802 - (MS15-009) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0025

Update Details

Recommendation is updated

17803 - (MS15-009) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0026

Update Details

Recommendation is updated

17804 - (MS15-009) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0027

Update Details

Recommendation is updated

17805 - (MS15-009) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0028

Update Details

Recommendation is updated

17806 - (MS15-009) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0029

Update Details

Recommendation is updated

17807 - (MS15-009) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0030

Update Details

Recommendation is updated

17808 - (MS15-009) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0031

Update Details

Recommendation is updated

17809 - (MS15-009) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0035

Update Details

Recommendation is updated

17810 - (MS15-009) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0036

Update Details

Recommendation is updated

17811 - (MS15-009) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0037

Update Details

Recommendation is updated

17812 - (MS15-009) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0038

Update Details

Recommendation is updated

17813 - (MS15-009) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0039

Update Details

Recommendation is updated

17814 - (MS15-009) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0040

Update Details

Recommendation is updated

17815 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0041

Update Details

Recommendation is updated

17818 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0044

Update Details

Recommendation is updated

17819 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0045

Update Details

Recommendation is updated

17820 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0046

Update Details

Recommendation is updated

17821 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0048

Update Details

Recommendation is updated

17822 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0049

Update Details

Recommendation is updated

17823 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0050

Update Details

Recommendation is updated

17825 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0052

Update Details

Recommendation is updated

17826 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0053

Update Details

Recommendation is updated

17829 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0066

Update Details

Recommendation is updated

17830 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0067

Update Details

Recommendation is updated

17831 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0068

Update Details

Recommendation is updated

17838 - (MS15-012) Vulnerability in Microsoft Office Could Allow Remote Code Execution (3032328)

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

Risk Level: High

CVE: CVE-2015-0063, CVE-2015-0064, CVE-2015-0065

Update Details

Recommendation is updated

17839 - (MS15-012) Microsoft Word OneTableDocumentStream Remote Code Execution (3032328)

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

Risk Level: High

CVE: CVE-2015-0065

Update Details

Recommendation is updated

17840 - (MS15-012) Microsoft Office Remote Code Execution (3032328)

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

Risk Level: High

CVE: CVE-2015-0064

Update Details

Recommendation is updated

17841 - (MS15-012) Microsoft Excel Remote Code Execution (3032328)

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

Risk Level: High

CVE: CVE-2015-0063

Update Details

Recommendation is updated

17854 - (MS15-010) Microsoft Windows TrueType Font Parsing Remote Code Execution (3036220)

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

Risk Level: High

CVE: CVE-2015-0059

Update Details

Recommendation is updated

17974 - (MS15-022) Vulnerabilities in Microsoft Office could allow Elevation of Privilege (3038999)

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

Risk Level: High

CVE: CVE-2015-0085, CVE-2015-0086, CVE-2015-0097, CVE-2015-1633, CVE-2015-1636

Update Details

Recommendation is updated

17987 - (MS15-022) Microsoft Office RTF Handling Remote Code Execution (3038999)

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

Risk Level: High

CVE: CVE-2015-0086

Update Details

Recommendation is updated

18011 - (MS15-018) Cumulative Security Update for Internet Explorer (3032359)

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

Risk Level: High

CVE: CVE-2015-0032, CVE-2015-0056, CVE-2015-0072, CVE-2015-0099, CVE-2015-0100, CVE-2015-1622, CVE-2015-1623, CVE-2015-1624, CVE-2015-1625, CVE-2015-1626, CVE-2015-1627, CVE-2015-1634

Update Details

Recommendation is updated

18013 - (MS15-018) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-0056

Update Details

Recommendation is updated

18015 - (MS15-018) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-0099

Update Details

Recommendation is updated

18016 - (MS15-018) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-0100

Update Details

Recommendation is updated

18017 - (MS15-018) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-1622

Update Details

Recommendation is updated

18018 - (MS15-018) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-1634

Update Details

Recommendation is updated

18019 - (MS15-018) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-1623

Update Details

Recommendation is updated

18020 - (MS15-018) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-1624

Update Details

Recommendation is updated

18021 - (MS15-018) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-1625

Update Details

Recommendation is updated

18022 - (MS15-018) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-1626

Update Details

Recommendation is updated

18023 - (MS15-018) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3032359)

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

Risk Level: High

CVE: CVE-2015-0032

Update Details

Recommendation is updated

18138 - (MS15-032) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1652

Update Details

Recommendation is updated

18139 - (MS15-032) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3038314)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1657

Update Details

Recommendation is updated

18140 - (MS15-032) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1659

Update Details

Recommendation is updated

18141 - (MS15-032) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1660

Update Details

Recommendation is updated

18143 - (MS15-032) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1662

Update Details

Recommendation is updated

18144 - (MS15-032) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1665

Update Details

Recommendation is updated

18145 - (MS15-032) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1666

Update Details

Recommendation is updated

18146 - (MS15-032) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1667

Update Details

Recommendation is updated

18147 - (MS15-032) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3038314)

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

Risk Level: High

CVE: CVE-2015-1668

Update Details

Recommendation is updated

18152 - (MS15-033) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)

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

Risk Level: High

CVE: CVE-2015-1639, CVE-2015-1641, CVE-2015-1642, CVE-2015-1649, CVE-2015-1650, CVE-2015-1651

Update Details

Recommendation is updated

18154 - (MS15-033) Microsoft Office Component Use-After-Free Remote Code Execution IV (3048019)

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

Risk Level: High

CVE: CVE-2015-1651

Update Details

Recommendation is updated

18155 - (MS15-033) Microsoft Office Component Use-After-Free Remote Code Execution III (3048019)

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

Risk Level: High

CVE: CVE-2015-1650

Update Details

Recommendation is updated

18156 - (MS15-033) Microsoft Office Component Use-After-Free Remote Code Execution II (3048019)

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

Risk Level: High

CVE: CVE-2015-1649

Update Details

Recommendation is updated

18158 - (MS15-033) Microsoft Office Memory Corruption Remote Code Execution (3048019)

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

Risk Level: High

CVE: CVE-2015-1641

Update Details

Recommendation is updated

18159 - (MS15-032) Cumulative Security Update for Internet Explorer (3038314)

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

Risk Level: High

CVE: CVE-2015-1652, CVE-2015-1657, CVE-2015-1659, CVE-2015-1660, CVE-2015-1661, CVE-2015-1662, CVE-2015-1665, CVE-2015-1666, CVE-2015-1667, CVE-2015-1668

Update Details

Recommendation is updated

18169 - (MS15-033) Microsoft Office Memory Corruption Remote Code Execution (3048019)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-1641

Update Details

Recommendation is updated

18263 - (MS15-046) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3057181)

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

Risk Level: High

CVE: CVE-2015-1682, CVE-2015-1683

Update Details

Recommendation is updated

18266 - (MS15-043) Cumulative Security Update for Internet Explorer (3049563)

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

Risk Level: High

CVE: CVE-2015-1658, CVE-2015-1684, CVE-2015-1685, CVE-2015-1686, CVE-2015-1688, CVE-2015-1689, CVE-2015-1691, CVE-2015-1692, CVE-2015-1694, CVE-2015-1703, CVE-2015-1704, CVE-2015-1705, CVE-2015-1706, CVE-2015-1708, CVE-2015-1709, CVE-2015-1710, CVE-2015-1711, CVE-2015-1712, CVE-2015-1713, CVE-2015-1714

Update Details

Recommendation is updated

18268 - (MS15-046) Microsoft Office Memory Corruption II Remote Code Execution (3057181)

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

Risk Level: High

CVE: CVE-2015-1683

Update Details

Recommendation is updated

18269 - (MS15-044) Vulnerabilities in GDI+ Could Allow Remote Code Execution (3057110)

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

Risk Level: High

CVE: CVE-2015-1670, CVE-2015-1671

Update Details

Recommendation is updated

18279 - (MS15-045) Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, CVE-2015-1699

Update Details

Recommendation is updated

18283 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3049563)

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

Risk Level: High

CVE: CVE-2015-1658

Update Details

Recommendation is updated

18288 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3049563)

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

Risk Level: High

CVE: CVE-2015-1689

Update Details

Recommendation is updated

18289 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3049563)

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

Risk Level: High

CVE: CVE-2015-1691

Update Details

Recommendation is updated

18292 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3049563)

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

Risk Level: High

CVE: CVE-2015-1694

Update Details

Recommendation is updated

18295 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3049563)

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

Risk Level: High

CVE: CVE-2015-1705

Update Details

Recommendation is updated

18296 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3049563)

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

Risk Level: High

CVE: CVE-2015-1706

Update Details

Recommendation is updated

18297 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3049563)

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

Risk Level: High

CVE: CVE-2015-1708

Update Details

Recommendation is updated

18298 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3049563)

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

Risk Level: High

CVE: CVE-2015-1709

Update Details

Recommendation is updated

18300 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3049563)

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

Risk Level: High

CVE: CVE-2015-1710

Update Details

Recommendation is updated

18301 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3049563)

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

Risk Level: High

CVE: CVE-2015-1711

Update Details

Recommendation is updated

18302 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3049563)

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

Risk Level: High

CVE: CVE-2015-1712

Update Details

Recommendation is updated

18304 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3049563)

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

Risk Level: High

CVE: CVE-2015-1714

Update Details

Recommendation is updated

18306 - (MS15-044) Microsoft Windows GDI+ TrueType Font Parsing Remote Code Execution (3057110)

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

Risk Level: High

CVE: CVE-2015-1671

Update Details

Recommendation is updated

18323 - (MS15-045) Microsoft Windows Journal I Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1675

Update Details

Recommendation is updated

18324 - (MS15-045) Microsoft Windows Journal II Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1695

Update Details

Recommendation is updated

18325 - (MS15-045) Microsoft Windows Journal III Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1696

Update Details

Recommendation is updated

18326 - (MS15-045) Microsoft Windows Journal IV Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1697

Update Details

Recommendation is updated

18327 - (MS15-045) Microsoft Windows Journal V Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1698

Update Details

Recommendation is updated

18328 - (MS15-045) Microsoft Windows Journal VI Remote Code Execution (3046002)

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

Risk Level: High

CVE: CVE-2015-1699

Update Details

Recommendation is updated

18335 - (MS15-044) Microsoft Windows GDI+ TrueType Font Parsing Remote Code Execution (3057110)

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

Risk Level: High

CVE: CVE-2015-1671

Update Details

Recommendation is updated

18339 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3049563)

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

Risk Level: High

CVE: CVE-2015-1717

Update Details

Recommendation is updated

18340 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3049563)

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

Risk Level: High

CVE: CVE-2015-1718

Update Details

Recommendation is updated

18425 - (MS15-056) Cumulative Security Update for Internet Explorer (3058515)

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

Risk Level: High

CVE: CVE-2015-1687, CVE-2015-1730, CVE-2015-1731, CVE-2015-1732, CVE-2015-1735, CVE-2015-1736, CVE-2015-1737, CVE-2015-1739, CVE-2015-1740, CVE-2015-1741, CVE-2015-1742, CVE-2015-1743, CVE-2015-1744, CVE-2015-1745, CVE-2015-1747, CVE-2015-1748, CVE-2015-1750, CVE-2015-1751, CVE-2015-1752, CVE-2015-1753, CVE-2015-1754, CVE-2015-1755, CVE-2015-1765, CVE-2015-1766

Update Details

Recommendation is updated

18427 - (MS15-056) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1766

Update Details

Recommendation is updated

18429 - (MS15-056) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1755

Update Details

Recommendation is updated

18430 - (MS15-056) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1754

Update Details

Recommendation is updated

18431 - (MS15-056) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1753

Update Details

Recommendation is updated

18432 - (MS15-056) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1752

Update Details

Recommendation is updated

18433 - (MS15-056) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1751

Update Details

Recommendation is updated

18434 - (MS15-056) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1750

Update Details

Recommendation is updated

18436 - (MS15-056) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1747

Update Details

Recommendation is updated

18437 - (MS15-056) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1745

Update Details

Recommendation is updated

18438 - (MS15-056) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1744

Update Details

Recommendation is updated

18440 - (MS15-056) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1742

Update Details

Recommendation is updated

18441 - (MS15-056) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1741

Update Details

Recommendation is updated

18442 - (MS15-056) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1740

Update Details

Recommendation is updated

18445 - (MS15-056) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1737

Update Details

Recommendation is updated

18446 - (MS15-056) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1736

Update Details

Recommendation is updated

18447 - (MS15-056) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1735

Update Details

Recommendation is updated

18449 - (MS15-056) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1732

Update Details

Recommendation is updated

18450 - (MS15-056) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1731

Update Details

Recommendation is updated

18451 - (MS15-056) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1730

Update Details

Recommendation is updated

18452 - (MS15-056) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1687

Update Details

Recommendation is updated

18453 - (MS15-059) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3064949)

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

Risk Level: High

CVE: CVE-2015-1759, CVE-2015-1760, CVE-2015-1770

Update Details

Recommendation is updated

18454 - (MS15-059) Microsoft Office Use-After-Free Remote Code Execution I (3064949)

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

Risk Level: High

CVE: CVE-2015-1759

Update Details

Recommendation is updated

18455 - (MS15-059) Microsoft Office Use-After-Free Remote Code Execution II (3064949)

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

Risk Level: High

CVE: CVE-2015-1760

Update Details

Recommendation is updated

18456 - (MS15-059) Microsoft Office Uninitialized Memory Use Remote Code Execution (3064949)

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

Risk Level: High

CVE: CVE-2015-1770

Update Details

Recommendation is updated

18558 - (HT204942) Apple OS X Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2014-8127, CVE-2014-8128, CVE-2014-8129, CVE-2014-8130, CVE-2014-8139, CVE-2014-8140, CVE-2014-8141, CVE-2015-0209, CVE-2015-0235, CVE-2015-0273, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0293, CVE-2015-1157, CVE-2015-1798, CVE-2015-1799, CVE-2015-3661, CVE-2015-3662, CVE-2015-3663, CVE-2015-3666, CVE-2015-3667, CVE-2015-3668, CVE-2015-3671, CVE-2015-3672, CVE-2015-3673, CVE-2015-3674, CVE-2015-3675, CVE-2015-3676, CVE-2015-3677, CVE-2015-3678, CVE-2015-3679, CVE-2015-3680, CVE-2015-3681, CVE-2015-3682, CVE-2015-3683, CVE-2015-3684, CVE-2015-3685, CVE-2015-3686, CVE-2015-3687, CVE-2015-3688, CVE-2015-3689, CVE-2015-3690, CVE-2015-3691, CVE-2015-3692, CVE-2015-3693, CVE-2015-3694, CVE-2015-3695, CVE-2015-3696, CVE-2015-3697, CVE-2015-3698, CVE-2015-3699, CVE-2015-3700, CVE-2015-3701, CVE-2015-3702, CVE-2015-3703, CVE-2015-3704, CVE-2015-3705, CVE-2015-3706, CVE-2015-3707, CVE-2015-3708, CVE-2015-3709, CVE-2015-3710, CVE-2015-3711, CVE-2015-3712, CVE-2015-3713, CVE-2015-3714, CVE-2015-3715, CVE-2015-3716, CVE-2015-3717, CVE-2015-3718, CVE-2015-3719, CVE-2015-3720, CVE-2015-3721, CVE-2015-4000, CVE-2015-7036

Update Details

CVE is updated

18608 - (MS15-070) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)

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

Risk Level: High

CVE: CVE-2015-2375, CVE-2015-2376, CVE-2015-2377, CVE-2015-2378, CVE-2015-2379, CVE-2015-2380, CVE-2015-2415, CVE-2015-2424

Update Details

Recommendation is updated

18611 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution V (3072620)

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

Risk Level: High

CVE: CVE-2015-2415

Update Details

Recommendation is updated

18612 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution IV (3072620)

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

Risk Level: High

CVE: CVE-2015-2380

Update Details

Recommendation is updated

18613 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution III (3072620)

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

Risk Level: High

CVE: CVE-2015-2379

Update Details

Recommendation is updated

18614 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution II (3072620)

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

Risk Level: High

CVE: CVE-2015-2377

Update Details

Recommendation is updated

18615 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution I (3072620)

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

Risk Level: High

CVE: CVE-2015-2376

Update Details

Recommendation is updated

18620 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3076321)

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

Risk Level: High

CVE: CVE-2015-1733

Update Details

Recommendation is updated

18621 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3076321)

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

Risk Level: High

CVE: CVE-2015-1738

Update Details

Recommendation is updated

18623 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3076321)

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

Risk Level: High

CVE: CVE-2015-1767

Update Details

Recommendation is updated

18624 - (MS15-065) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3076321)

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

Risk Level: High

CVE: CVE-2015-2372

Update Details

Recommendation is updated

18626 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3076321)

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

Risk Level: High

CVE: CVE-2015-2383

Update Details

Recommendation is updated

18627 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3076321)

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

Risk Level: High

CVE: CVE-2015-2384

Update Details

Recommendation is updated

18628 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3076321)

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

Risk Level: High

CVE: CVE-2015-2385

Update Details

Recommendation is updated

18629 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3076321)

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

Risk Level: High

CVE: CVE-2015-2388

Update Details

Recommendation is updated

18630 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3076321)

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

Risk Level: High

CVE: CVE-2015-2389

Update Details

Recommendation is updated

18631 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3076321)

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

Risk Level: High

CVE: CVE-2015-2390

Update Details

Recommendation is updated

18632 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3076321)

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

Risk Level: High

CVE: CVE-2015-2391

Update Details

Recommendation is updated

18633 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3076321)

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

Risk Level: High

CVE: CVE-2015-2397

Update Details

Recommendation is updated

18635 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3076321)

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

Risk Level: High

CVE: CVE-2015-2401

Update Details

Recommendation is updated

18636 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3076321)

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

Risk Level: High

CVE: CVE-2015-2403

Update Details

Recommendation is updated

18637 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3076321)

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

Risk Level: High

CVE: CVE-2015-2404

Update Details

Recommendation is updated

18638 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XV (3076321)

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

Risk Level: High

CVE: CVE-2015-2406

Update Details

Recommendation is updated

18640 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVI (3076321)

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

Risk Level: High

CVE: CVE-2015-2408

Update Details

Recommendation is updated

18643 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVII (3076321)

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

Risk Level: High

CVE: CVE-2015-2411

Update Details

Recommendation is updated

18647 - (MS15-065) Microsoft Internet Explorer JScript9 Memory Corruption Remote Code Execution (3076321)

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

Risk Level: High

CVE: CVE-2015-2419

Update Details

Recommendation is updated

18649 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVIII (3076321)

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

Risk Level: High

CVE: CVE-2015-2422

Update Details

Recommendation is updated

18657 - (MS15-070) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)

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

Risk Level: High

CVE: CVE-2015-2375, CVE-2015-2376, CVE-2015-2377, CVE-2015-2378, CVE-2015-2379, CVE-2015-2380, CVE-2015-2415, CVE-2015-2424

Update Details

Recommendation is updated

18762 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3082442)

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

Risk Level: High

CVE: CVE-2015-2441

Update Details

Recommendation is updated

18763 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3082442)

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

Risk Level: High

CVE: CVE-2015-2442

Update Details

Recommendation is updated

18764 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3082442)

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

Risk Level: High

CVE: CVE-2015-2443

Update Details

Recommendation is updated

18765 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3082442)

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

Risk Level: High

CVE: CVE-2015-2444

Update Details

Recommendation is updated

18766 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3082442)

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

Risk Level: High

CVE: CVE-2015-2446

Update Details

Recommendation is updated

18767 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3082442)

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

Risk Level: High

CVE: CVE-2015-2447

Update Details

Recommendation is updated

18768 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3082442)

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

Risk Level: High

CVE: CVE-2015-2448

Update Details

Recommendation is updated

18769 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3082442)

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

Risk Level: High

CVE: CVE-2015-2450

Update Details

Recommendation is updated

18770 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3082442)

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

Risk Level: High

CVE: CVE-2015-2451

Update Details

Recommendation is updated

18771 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3082442)

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

Risk Level: High

CVE: CVE-2015-2452

Update Details

Recommendation is updated

18781 - (MS15-079) Cumulative Security Update for Internet Explorer (3082442)

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

Risk Level: High

CVE: CVE-2015-2423, CVE-2015-2441, CVE-2015-2442, CVE-2015-2443, CVE-2015-2444, CVE-2015-2445, CVE-2015-2446, CVE-2015-2447, CVE-2015-2448, CVE-2015-2449, CVE-2015-2450, CVE-2015-2451, CVE-2015-2452

Update Details

Recommendation is updated

18782 - (MS15-080) Microsoft Office Graphics Component Remote Code Execution (3078662)

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

Risk Level: High

CVE: CVE-2015-2431

Update Details

Recommendation is updated

18783 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution I (3078662)

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

Risk Level: High

CVE: CVE-2015-2432

Update Details

Recommendation is updated

18784 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution I (3078662)

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

Risk Level: High

CVE: CVE-2015-2435

Update Details

Recommendation is updated

18785 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution II (3078662)

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

Risk Level: High

CVE: CVE-2015-2455

Update Details

Recommendation is updated

18786 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution III (3078662)

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

Risk Level: High

CVE: CVE-2015-2456

Update Details

Recommendation is updated

18787 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution II (3078662)

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

Risk Level: High

CVE: CVE-2015-2458

Update Details

Recommendation is updated

18788 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution III (3078662)

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

Risk Level: High

CVE: CVE-2015-2459

Update Details

Recommendation is updated

18789 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution IV (3078662)

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

Risk Level: High

CVE: CVE-2015-2460

Update Details

Recommendation is updated

18790 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution V (3078662)

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

Risk Level: High

CVE: CVE-2015-2461

Update Details

Recommendation is updated

18791 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution VI (3078662)

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

Risk Level: High

CVE: CVE-2015-2462

Update Details

Recommendation is updated

18792 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution IV (3078662)

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

Risk Level: High

CVE: CVE-2015-2463

Update Details

Recommendation is updated

18793 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution V (3078662)

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

Risk Level: High

CVE: CVE-2015-2464

Update Details

Recommendation is updated

18797 - (MS15-081) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1642, CVE-2015-2423, CVE-2015-2466, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2470, CVE-2015-2477

Update Details

Recommendation is updated

18801 - (MS15-091) Microsoft Edge Memory Corruption I Remote Code Execution (3084525)

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

Risk Level: High

CVE: CVE-2015-2441

Update Details

Recommendation is updated

18802 - (MS15-091) Microsoft Edge Memory Corruption II Remote Code Execution (3084525)

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

Risk Level: High

CVE: CVE-2015-2442

Update Details

Recommendation is updated

18803 - (MS15-091) Microsoft Edge Memory Corruption III Remote Code Execution (3084525)

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

Risk Level: High

CVE: CVE-2015-2446

Update Details

Recommendation is updated

18805 - (MS15-080) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)

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

Risk Level: High

CVE: CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465

Update Details

Recommendation is updated

18808 - (MS15-091) Cumulative Security Update for Microsoft Edge (3084525)

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

Risk Level: High

CVE: CVE-2015-2441, CVE-2015-2442, CVE-2015-2446, CVE-2015-2449

Update Details

Recommendation is updated

18810 - (MS15-080) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)

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

Risk Level: High

CVE: CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465

Update Details

Recommendation is updated

18820 - (MS15-092) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3086251)

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

Risk Level: High

CVE: CVE-2015-2479, CVE-2015-2480, CVE-2015-2481

Update Details

Recommendation is updated

18822 - (MS15-081) Microsoft Office Memory Corruption I Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-1642

Update Details

Recommendation is updated

18824 - (MS15-081) Microsoft Office Memory Corruption II Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2466

Update Details

Recommendation is updated

18825 - (MS15-081) Microsoft Office Memory Corruption III Remote Code Execution (3080790)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2467

Update Details

Recommendation is updated

18826 - (MS15-081) Microsoft Office Memory Corruption IV Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2468

Update Details

Recommendation is updated

18827 - (MS15-081) Microsoft Office Memory Corruption V Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2469

Update Details

Recommendation is updated

18828 - (MS15-081) Microsoft Office Memory Corruption Integer Underflow Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2470

Update Details

Recommendation is updated

18829 - (MS15-081) Microsoft Office Memory Corruption VI Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2477

Update Details

Recommendation is updated

18835 - (MS15-092) Microsoft .NET Framework RyuJIT Optimization Privilege Escalation I (3086251)

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

Risk Level: High

CVE: CVE-2015-2479

Update Details

Recommendation is updated

18836 - (MS15-092) Microsoft .NET Framework RyuJIT Optimization Privilege Escalation II (3086251)

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

Risk Level: High

CVE: CVE-2015-2480

Update Details

Recommendation is updated

18837 - (MS15-092) Microsoft .NET Framework RyuJIT Optimization Privilege Escalation III (3086251)

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

Risk Level: High

CVE: CVE-2015-2481

Update Details

Recommendation is updated

18838 - (MS15-081) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-1642, CVE-2015-2423, CVE-2015-2466, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2470, CVE-2015-2477

Update Details

Recommendation is updated

18846 - (MS15-093) Microsoft Internet Explorer Memory Corruption Remote Code Execution (3088903)

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

Risk Level: High

CVE: CVE-2015-2502

Update Details

Recommendation is updated

18919 - (MS15-101) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)

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

Risk Level: High

CVE: CVE-2015-2504

Update Details

Recommendation is updated

18920 - (MS15-101) Microsoft .NET Framework Object Copy Privilege Escalation (3089662)

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

Risk Level: High

CVE: CVE-2015-2504

Update Details

Recommendation is updated

18928 - (MS15-094) Cumulative Security Update for Internet Explorer (3089548)

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

Risk Level: High

CVE: CVE-2015-2483, CVE-2015-2484, CVE-2015-2485, CVE-2015-2486, CVE-2015-2487, CVE-2015-2489, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2498, CVE-2015-2499, CVE-2015-2500, CVE-2015-2501, CVE-2015-2541, CVE-2015-2542

Update Details

Recommendation is updated

18929 - (MS15-094) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2486

Update Details

Recommendation is updated

18930 - (MS15-094) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2485

Update Details

Recommendation is updated

18933 - (MS15-094) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2490

Update Details

Recommendation is updated

18935 - (MS15-094) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2487

Update Details

Recommendation is updated

18936 - (MS15-094) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2499

Update Details

Recommendation is updated

18937 - (MS15-094) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2498

Update Details

Recommendation is updated

18938 - (MS15-094) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2492

Update Details

Recommendation is updated

18939 - (MS15-094) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2491

Update Details

Recommendation is updated

18940 - (MS15-094) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2542

Update Details

Recommendation is updated

18941 - (MS15-094) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2541

Update Details

Recommendation is updated

18942 - (MS15-094) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2501

Update Details

Recommendation is updated

18943 - (MS15-094) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2500

Update Details

Recommendation is updated

18944 - (MS15-099) Microsoft Office Memory Corruption III Remote Code Execution (3089664)

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

Risk Level: High

CVE: CVE-2015-2523

Update Details

Recommendation is updated

18946 - (MS15-099) Microsoft Office Memory Corruption II Remote Code Execution (3089664)

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

Risk Level: High

CVE: CVE-2015-2521

Update Details

Recommendation is updated

18947 - (MS15-099) Microsoft Office Memory Corruption I Remote Code Execution (3089664)

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

Risk Level: High

CVE: CVE-2015-2520

Update Details

Recommendation is updated

18948 - (MS15-099) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)

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

Risk Level: High

CVE: CVE-2015-2520, CVE-2015-2521, CVE-2015-2522, CVE-2015-2523

Update Details

Recommendation is updated

18949 - (MS15-099) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)

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

Risk Level: High

CVE: CVE-2015-2520, CVE-2015-2521, CVE-2015-2522, CVE-2015-2523

Update Details

Recommendation is updated

18960 - (MS15-097) Microsoft Windows Graphics OpenType Font Parsing Denial of Service (3089656)

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

Risk Level: High

CVE: CVE-2015-2506

Update Details

Recommendation is updated

18963 - (MS15-097) Microsoft Windows Graphics Font Parsing Remote Code Execution (3089656)

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

Risk Level: High

CVE: CVE-2015-2510

Update Details

Recommendation is updated

18969 - (MS15-094) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2494

Update Details

Recommendation is updated

18970 - (MS15-094) Microsoft Internet Explorer Scripting Engine Remote Code Execution(3089548)

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

Risk Level: High

CVE: CVE-2015-2493

Update Details

Recommendation is updated

18973 - (MS15-098) Microsoft Windows Journal I Remote Code Execution (3089669)

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

Risk Level: High

CVE: CVE-2015-2513

Update Details

Recommendation is updated

18974 - (MS15-098) Microsoft Windows Journal II Remote Code Execution (3089669)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2514

Update Details

Recommendation is updated

18976 - (MS15-098) Microsoft Windows Journal Remote Code Execution (3089669)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2519

Update Details

Recommendation is updated

18977 - (MS15-098) Microsoft Windows Journal III Remote Code Execution (3089669)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2530

Update Details

Recommendation is updated

18978 - (MS15-095) Microsoft Edge Memory Corruption I Remote Code Execution (3089665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2485

Update Details

Recommendation is updated

18979 - (MS15-095) Microsoft Edge Memory Corruption II Remote Code Execution (3089665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2486

Update Details

Recommendation is updated

18980 - (MS15-095) Microsoft Edge Memory Corruption III Remote Code Execution (3089665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2494

Update Details

Recommendation is updated

18981 - (MS15-095) Microsoft Edge Memory Corruption IV Remote Code Execution (3089665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2542

Update Details

Recommendation is updated

18983 - (MS15-095) Cumulative Security Update for Microsoft Edge (3089665)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2485, CVE-2015-2486, CVE-2015-2494, CVE-2015-2542

Update Details

Recommendation is updated

18984 - (MS15-097) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2506, CVE-2015-2507, CVE-2015-2508, CVE-2015-2510, CVE-2015-2511, CVE-2015-2512, CVE-2015-2517, CVE-2015-2518, CVE-2015-2527, CVE-2015-2529, CVE-2015-2546

Update Details

Recommendation is updated

18985 - (MS15-098) Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2513, CVE-2015-2514, CVE-2015-2516, CVE-2015-2519, CVE-2015-2530

Update Details

Recommendation is updated

18989 - (MS15-099) Microsoft Office Malformed EPS File Remote Code Execution (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2545

Update Details

Recommendation is updated

19077 - (MS15-109) Security Update for Windows Shell to Address Remote Code Execution (3096443)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2515, CVE-2015-2548

Update Details

Recommendation is updated

19078 - (MS15-109) Microsoft Windows Toolbar Use-After Free Remote Code Execution (3096443)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2515

Update Details

Recommendation is updated

19079 - (MS15-109) Microsoft Windows Tablet Input Band Use-After Free Remote Code Execution (3096443)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2548

Update Details

Recommendation is updated

19080 - (MS15-106) Microsoft Internet Explorer Scripting Engine Memory Corruption I Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2482

Update Details

Recommendation is updated

19081 - (MS15-106) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6042

Update Details

Recommendation is updated

19082 - (MS15-110) Microsoft Office Memory Corruption Remote Code Execution I (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2555

Update Details

Recommendation is updated

19089 - (MS15-106) Microsoft Internet Explorer Memory Corruption Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6048

Update Details

Recommendation is updated

19090 - (MS15-106) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6049

Update Details

Recommendation is updated

19091 - (MS15-106) Microsoft Internet Explorer Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6050

Update Details

Recommendation is updated

19095 - (MS15-106) Microsoft Internet Explorer Scripting Engine Memory Corruption II Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6055

Update Details

Recommendation is updated

19096 - (MS15-106) Microsoft Internet Explorer Scripting Engine Memory Corruption III Remote Code Execution (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6056

Update Details

Recommendation is updated

19103 - (MS15-106) Cumulative Security Update for Internet Explorer (3096441)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2482, CVE-2015-6042, CVE-2015-6043, CVE-2015-6044, CVE-2015-6045, CVE-2015-6046, CVE-2015-6047, CVE-2015-6048, CVE-2015-6049, CVE-2015-6050, CVE-2015-6051, CVE-2015-6052, CVE-2015-6053, CVE-2015-6055, CVE-2015-6056, CVE-2015-6059

Update Details

Recommendation is updated

19105 - (MS15-110) Microsoft Office Memory Corruption Remote Code Execution II (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2557

Update Details

Recommendation is updated

19106 - (MS15-110) Microsoft Office Memory Corruption Remote Code Execution III (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2558

Update Details

Recommendation is updated

19109 - (MS15-110) Security Updates for Microsoft Office to Address Remote Code Execution

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2555, CVE-2015-2556, CVE-2015-2557, CVE-2015-2558, CVE-2015-6037, CVE-2015-6039

Update Details

Recommendation is updated

19120 - (MS15-110) Security Updates for Microsoft Office to Address Remote Code Execution

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-2555, CVE-2015-2556, CVE-2015-2557, CVE-2015-2558, CVE-2015-6037, CVE-2015-6039

Update Details

Recommendation is updated

19206 - (MS15-116) Microsoft Office COM Control Privilege Escalation (3104540)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2503

Update Details

Recommendation is updated Risk is updated

19207 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution V (3104540)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6038

Update Details

Recommendation is updated Risk is updated

19208 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution I (3104540)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6091

Update Details

Recommendation is updated Risk is updated

19209 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution II (3104540)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6092

Update Details

Recommendation is updated Risk is updated

19210 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution III (3104540)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6093

Update Details

Recommendation is updated Risk is updated

19211 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution IV (3104540)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6094

Update Details

Recommendation is updated Risk is updated

19214 - (MS15-114) Microsoft Windows Journal Heap Overflow Remote Code Execution (3100213)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6097

Update Details

Recommendation is updated

19216 - (MS15-114) Security Update for Windows Journal to Address Remote Code Execution (3100213)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6097

Update Details

Recommendation is updated Risk is updated

19218 - (MS15-113) Cumulative Security Update for Microsoft Edge (3104519)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6064, CVE-2015-6073, CVE-2015-6078, CVE-2015-6088

Update Details

Recommendation is updated

19219 - (MS15-113) Microsoft Edge Memory Corruption Remote Code Execution III (3104519)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6078

Update Details

Recommendation is updated

19220 - (MS15-113) Microsoft Edge Memory Corruption Remote Code Execution II (3104519)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6073

Update Details

Recommendation is updated

19222 - (MS15-113) Microsoft Edge Memory Corruption Remote Code Execution I (3104519)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6064

Update Details

Recommendation is updated

19223 - (MS15-115) Security Update for Microsoft Windows to Address Remote Code Execution (3105864)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6100, CVE-2015-6101, CVE-2015-6102, CVE-2015-6103, CVE-2015-6104, CVE-2015-6109, CVE-2015-6113

Update Details

Recommendation is updated

19227 - (MS15-115) Microsoft Windows Adobe Type Manager Library OpenType Fonts Remote Code Execution I (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6103

Update Details

Recommendation is updated

19228 - (MS15-115) Microsoft Windows Adobe Type Manager Library OpenType Fonts Remote Code Execution II (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6104

Update Details

Recommendation is updated

19242 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2427

Update Details

Recommendation is updated

19243 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6064

Update Details

Recommendation is updated

19244 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6065

Update Details

Recommendation is updated

19245 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6066

Update Details

Recommendation is updated

19246 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6068

Update Details

Recommendation is updated

19247 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6069

Update Details

Recommendation is updated

19248 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6070

Update Details

Recommendation is updated

19249 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6071

Update Details

Recommendation is updated

19250 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6073

Update Details

Recommendation is updated

19251 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6074

Update Details

Recommendation is updated

19252 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6075

Update Details

Recommendation is updated

19253 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6076

Update Details

Recommendation is updated

19254 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6077

Update Details

Recommendation is updated

19255 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XV (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6078

Update Details

Recommendation is updated

19256 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVI (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6079

Update Details

Recommendation is updated

19257 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6080

Update Details

Recommendation is updated

19258 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVIII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6081

Update Details

Recommendation is updated

19259 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIX (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6082

Update Details

Recommendation is updated

19260 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XX (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6084

Update Details

Recommendation is updated

19261 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXI (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6085

Update Details

Recommendation is updated

19263 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXII (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6087

Update Details

Recommendation is updated

19265 - (MS15-112) Microsoft Internet Explorer Scripting Engine Remote Code Execution (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6089

Update Details

Recommendation is updated

19266 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6072

Update Details

Recommendation is updated

19267 - (MS15-112) Cumulative Security Update for Internet Explorer (3104517)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2427, CVE-2015-6064, CVE-2015-6065, CVE-2015-6066, CVE-2015-6068, CVE-2015-6069, CVE-2015-6070, CVE-2015-6071, CVE-2015-6072, CVE-2015-6073, CVE-2015-6074, CVE-2015-6075, CVE-2015-6076, CVE-2015-6077, CVE-2015-6078, CVE-2015-6079, CVE-2015-6080, CVE-2015-6081, CVE-2015-6082, CVE-2015-6084, CVE-2015-6085, CVE-2015-6086, CVE-2015-6087, CVE-2015-6088, CVE-2015-6089

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

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

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

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

5515 - (MS07-058) Microsoft Windows RPC Authentication Vulnerability Could Allow Denial of Service (933729)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2228

Update Details

Recommendation is updated

5530 - (MS07-058) Microsoft Windows RPC Authentication Vulnerability Could Allow Denial of Service (933729) - No Credentials Required

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2007-2228

Update Details

Recommendation is updated

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 WordRTF Object Parsing Vulnerability (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4025

Update Details

Recommendation is updated

6282 - (MS08-072) Microsoft Word Memory Corruption Remote Code Execution (957173)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4026

Update Details

Recommendation is updated

6419 - (MS09-005) Microsoft Visio Memory Corruption Vulnerability - CVE-2009-0095 - (957634)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0095

Update Details

Recommendation is updated

6459 - (MS09-009) Microsoft Office Excel Memory Corruption Vulnerability II (968557)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0238

Update Details

Recommendation is updated

6492 - (MS09-006) Microsoft Windows Kernel Input Validation Vulnerability (958690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0081

Update Details

Recommendation is updated

6595 - (MS09-009) Microsoft Office Excel Memory Corruption Vulnerability (968557)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0100

Update Details

Recommendation is updated

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

7546 - (MS09-027) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (969514)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0563, CVE-2009-0565

Update Details

Recommendation is updated

7624 - (MS08-019) Vulnerabilities In Microsoft Visio Could Allow Remote Code Execution (949032)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1089, CVE-2008-1090

Update Details

Recommendation is updated

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

8527 - (MS10-028) Microsoft Visio Attribute Validation Memory Corruption Vulnerability (980094)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0254

Update Details

Recommendation is updated

8528 - (MS10-028) Microsoft Visio Index Calculation Memory Corruption Vulnerability (980094)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0256

Update Details

Recommendation is updated

8534 - (MS10-023) Microsoft Office Publisher Conversion TextBox Processing Buffer Overflow Vulnerability (981160)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0479

Update Details

Recommendation is updated

8547 - (MS10-023) Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0479

Update Details

Recommendation is updated

9712 - (MS10-058) Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1892, CVE-2010-1893

Update Details

Recommendation is updated

10661 - (MS10-087) Microsoft Office DLL Planting Vulnerability (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3337

Update Details

Recommendation is updated

10662 - (MS10-087) Microsoft Office RTF Stack Buffer Overflow (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3333

Update Details

Recommendation is updated

10664 - (MS10-087) Microsoft Office Art Drawing Records (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3334

Update Details

Recommendation is updated

10665 - (MS10-087) Microsoft Office Drawing Exception Handling (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3335

Update Details

Recommendation is updated

10666 - (MS10-087) Microsoft Office MSO Large SPID Read AV (2423930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3336

Update Details

Recommendation is updated

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

12348 - (MS11-056) Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1281, CVE-2011-1282, CVE-2011-1283, CVE-2011-1284, CVE-2011-1870

Update Details

Recommendation is updated

13086 - (MS11-094) Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2639142)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3396, CVE-2011-3413

Update Details

Recommendation is updated

13292 - (MS12-008) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-5046, CVE-2012-0154

Update Details

Recommendation is updated

13552 - (MS09-027) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (969514)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2009-0563, CVE-2009-0565

Update Details

Recommendation is updated

13780 - (MS12-042) Microsoft Windows BIOS ROM Corruption Privilege Escalation (2711167)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1515

Update Details

Recommendation is updated

13787 - (MS12-042) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0217, CVE-2012-1515

Update Details

Recommendation is updated

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

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

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

5626 - (MS07-066) Microsoft Windows Kernel Vulnerability (943078)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5350

Update Details

Recommendation is updated

5805 - (MS08-025) Microsoft Windows Kernel Vulnerability (941693)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1084

Update Details

Recommendation is updated

6495 - (MS09-007) Microsoft Windows SChannel Spoofing Vulnerability (960225)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0085

Update Details

Recommendation is updated

7227 - (MS09-058) Vulnerabilities In Windows Kernel Could Allow Elevation of Privilege (971486)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2515, CVE-2009-2516, CVE-2009-2517

Update Details

Recommendation is updated

7316 - (MS09-065) Win32k NULL Pointer Dereferencing Vulnerability (969947)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1127

Update Details

Recommendation is updated

7317 - (MS09-065) Win32k Insufficient Data Validation Vulnerability (969947)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2513

Update Details

Recommendation is updated

7414 - (MS09-007) Vulnerability In SChannel Could Allow Spoofing (960225)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0085

Update Details

Recommendation is updated

7681 - (MS08-061)Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (954211)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2250, CVE-2008-2251, CVE-2008-2252

Update Details

Recommendation is updated

7732 - (MS08-025) Vulnerability In Windows Kernel Could Allow Elevation Of Privilege (941693)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1084

Update Details

Recommendation is updated

7860 - (MS10-015) Windows Kernel Exception Handler Vulnerability (977165)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0232

Update Details

Recommendation is updated

7861 - (MS10-015) Windows Kernel Double Free Vulnerability (977165)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0233

Update Details

Recommendation is updated

7889 - (MS10-015) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0232, CVE-2010-0233

Update Details

Recommendation is updated

8535 - (MS10-022) Microsoft VBScript Help Keypress Vulnerability (981169)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0483

Update Details

Recommendation is updated

8545 - (MS10-021) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0234, CVE-2010-0235, CVE-2010-0236, CVE-2010-0237, CVE-2010-0238, CVE-2010-0481, CVE-2010-0482, CVE-2010-0810

Update Details

Recommendation is updated

9680 - (MS10-058) Microsoft Windows IPv6 Memory Corruption Denial Of Service (978886)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1892

Update Details

Recommendation is updated

9694 - (MS10-048) Microsoft Windows Win32k Window Creation Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1897

Update Details

Recommendation is updated

9695 - (MS10-048) Microsoft Windows Win32k User Input Validation Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1896

Update Details

Recommendation is updated

9696 - (MS10-048) Microsoft Windows Win32k Exception Handling Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1894

Update Details

Recommendation is updated

9715 - (MS10-047) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1888, CVE-2010-1889, CVE-2010-1890

Update Details

Recommendation is updated

9722 - (MS10-048) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1887, CVE-2010-1894, CVE-2010-1895, CVE-2010-1896, CVE-2010-1897

Update Details

Recommendation is updated

10317 - (MS10-085) Vulnerability in SChannel Could Allow Denial of Service (2207566)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3229

Update Details

Recommendation is updated

10318 - (MS10-085) Microsoft Windows TLSv1 Denial of Service (2207566)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3229

Update Details

Recommendation is updated

10773 - (MS11-011) Windows Kernel Improper Data Validation (2393802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4398

Update Details

Recommendation is updated

10869 - (MS10-098) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3939, CVE-2010-3940, CVE-2010-3941, CVE-2010-3942, CVE-2010-3943, CVE-2010-3944

Update Details

Recommendation is updated

10898 - (MS10-098) Microsoft Windows Win32k Buffer Overflow Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2739, CVE-2010-3939

Update Details

Recommendation is updated

10899 - (MS10-098) Microsoft Windows Win32k Buffer Overflow Could Allow Elevation Of Privilege CVE-2010-3940 (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3940

Update Details

Recommendation is updated

10900 - (MS10-098) Microsoft Windows Win32k Double Free Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3941

Update Details

Recommendation is updated

10901 - (MS10-098) Microsoft Windows Win32k WriteAV Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3942

Update Details

Recommendation is updated

10902 - (MS10-098) Microsoft Windows Win32k Cursor Linking Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3943

Update Details

Recommendation is updated

10903 - (MS10-098) Microsoft Windows Win32k Memory Corruption Could Allow Elevation Of Privilege (2436673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3944

Update Details

Recommendation is updated

11224 - (MS11-013) Microsoft Kerberos Unkeyed Checksum (2496930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0043

Update Details

Recommendation is updated

11226 - (MS11-013) Vulnerabilities in Microsoft Kerberos Could Allow Elevation Of Privilege (2496930)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0043, CVE-2011-0091

Update Details

Recommendation is updated

11237 - (MS11-011) Windows Kernel Integer Truncation (2393802)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0045

Update Details

Recommendation is updated

11244 - (MS11-012) Microsoft Win32k Improper User Input Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0086

Update Details

Recommendation is updated

11245 - (MS11-012) Microsoft Win32k Insufficient User Input Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0087

Update Details

Recommendation is updated

11246 - (MS11-012) Microsoft Win32k Window Class Pointer Confusion (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0088

Update Details

Recommendation is updated

11247 - (MS11-012) Microsoft Win32k Window Class Improper Pointer Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0089

Update Details

Recommendation is updated

11248 - (MS11-012) Microsoft Win32k Memory Corruption (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0090

Update Details

Recommendation is updated

11253 - (MS11-011) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (2393802)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4398, CVE-2011-0045

Update Details

Recommendation is updated

11266 - (MS11-012) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2479628)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0086, CVE-2011-0087, CVE-2011-0088, CVE-2011-0089, CVE-2011-0090

Update Details

Recommendation is updated

11791 - (MS11-034) Microsoft Win32k Use After Free I (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0662

Update Details

Recommendation is updated

11792 - (MS11-034) Microsoft Win32k Use After Free II (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0665

Update Details

Recommendation is updated

11793 - (MS11-034) Microsoft Win32k Use After Free III (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0666

Update Details

Recommendation is updated

11794 - (MS11-034) Microsoft Win32k Use After Free IV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0667

Update Details

Recommendation is updated

11795 - (MS11-034) Microsoft Win32k Use After Free V (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0670

Update Details

Recommendation is updated

11796 - (MS11-034) Microsoft Win32k Use After Free VI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0671

Update Details

Recommendation is updated

11797 - (MS11-034) Microsoft Win32k Use After Free VII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0672

Update Details

Recommendation is updated

11798 - (MS11-034) Microsoft Win32k Use After Free VIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0674

Update Details

Recommendation is updated

11799 - (MS11-034) Microsoft Win32k Use After Free IX (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1234

Update Details

Recommendation is updated

11800 - (MS11-034) Microsoft Win32k Use After Free X (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1235

Update Details

Recommendation is updated

11801 - (MS11-034) Microsoft Win32k Use After Free XI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1236

Update Details

Recommendation is updated

11802 - (MS11-034) Microsoft Win32k Use After Free XII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1237

Update Details

Recommendation is updated

11803 - (MS11-034) Microsoft Win32k Use After Free XIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1238

Update Details

Recommendation is updated

11804 - (MS11-034) Microsoft Win32k Use After Free XIV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1239

Update Details

Recommendation is updated

11805 - (MS11-034) Microsoft Win32k Use After Free XV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1240

Update Details

Recommendation is updated

11806 - (MS11-034) Microsoft Win32k Use After Free XVI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1241

Update Details

Recommendation is updated

11807 - (MS11-034) Microsoft Win32k Use After Free XVII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1242

Update Details

Recommendation is updated

11808 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation I (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0673

Update Details

Recommendation is updated

11809 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation II (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0676

Update Details

Recommendation is updated

11810 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation III (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0677

Update Details

Recommendation is updated

11811 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation IV (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1225

Update Details

Recommendation is updated

11812 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation V (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1226

Update Details

Recommendation is updated

11813 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1227

Update Details

Recommendation is updated

11814 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1228

Update Details

Recommendation is updated

11815 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1229

Update Details

Recommendation is updated

11816 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation IX (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1230

Update Details

Recommendation is updated

11817 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation X (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1231

Update Details

Recommendation is updated

11818 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation XI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1232

Update Details

Recommendation is updated

11819 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation XII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1233

Update Details

Recommendation is updated

11836 - (MS11-034) Microsoft Win32k Use After Free XVIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0675

Update Details

Recommendation is updated

12221 - (MS11-046) Microsoft Windows Ancillary Function Driver Could Allow Elevation Of Privilege (2503665)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1249

Update Details

Recommendation is updated

12248 - (MS11-046) Microsoft Windows Ancillary Function Driver Could Allow Elevation Of Privilege (2503665)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1249

Update Details

Recommendation is updated

12324 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation I (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1874

Update Details

Recommendation is updated

12325 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation II (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1875

Update Details

Recommendation is updated

12326 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation III (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1876

Update Details

Recommendation is updated

12327 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation IV (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1877

Update Details

Recommendation is updated

12328 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation V (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1878

Update Details

Recommendation is updated

12329 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VI (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1879

Update Details

Recommendation is updated

12330 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation I (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1880

Update Details

Recommendation is updated

12331 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation II (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1881

Update Details

Recommendation is updated

12332 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VII (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1882

Update Details

Recommendation is updated

12333 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VIII (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1883

Update Details

Recommendation is updated

12334 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation IX (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1884

Update Details

Recommendation is updated

12335 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation III (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1885

Update Details

Recommendation is updated

12337 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation IV (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1887

Update Details

Recommendation is updated

12338 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation V (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1888

Update Details

Recommendation is updated

12341 - (MS11-056) Microsoft Windows CSRSS Local EOP AllocConsole Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1281

Update Details

Recommendation is updated

12342 - (MS11-054) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1874, CVE-2011-1875, CVE-2011-1876, CVE-2011-1877, CVE-2011-1878, CVE-2011-1879, CVE-2011-1880, CVE-2011-1881, CVE-2011-1882, CVE-2011-1883, CVE-2011-1884, CVE-2011-1885, CVE-2011-1886, CVE-2011-1887, CVE-2011-1888

Update Details

Recommendation is updated

12343 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvSetConsoleLocalEUDC Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1282

Update Details

Recommendation is updated

12344 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvSetConsoleNumberOfCommand Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1283

Update Details

Recommendation is updated

12345 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvWriteConsoleOutput Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1284

Update Details

Recommendation is updated

12346 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvWriteConsoleOutputString Privilege Escalation (2507938)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1870

Update Details

Recommendation is updated

12444 - (MS11-063) Microsoft WCRSS Could Allow Elevation Of Privilege (2567680)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1967

Update Details

Recommendation is updated

12445 - (MS11-063) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1967

Update Details

Recommendation is updated

12738 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k Null Pointer De-reference (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1985

Update Details

Recommendation is updated

12741 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k Use After Free (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2011

Update Details

Recommendation is updated

12913 - (MS11-084) Microsoft Windows TrueType Font Parsing Denial of Service (2617657)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2004

Update Details

Recommendation is updated

12914 - (MS11-084) Vulnerability in Microsoft Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2004

Update Details

Recommendation is updated

13055 - (MS11-097) Microsoft Windows CSRSS Local Privilege Elevation (2620712)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3408

Update Details

Recommendation is updated

13056 - (MS11-098) Microsoft Windows Kernel Exception Handler (2633171)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2018

Update Details

Recommendation is updated

13058 - (MS11-088) Microsoft Office Pinyin IME Privilege Escalation (2652016)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2010

Update Details

Recommendation is updated

13059 - (MS11-097) Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2620712)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3408

Update Details

Recommendation is updated

13060 - (MS11-098) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2018

Update Details

Recommendation is updated

13070 - (MS11-088) Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2652016)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2010

Update Details

Recommendation is updated

13158 - (MS11-100) Microsoft Windows .NET Hash Tables Denial of Service (2659883)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3414

Update Details

Recommendation is updated

13290 - (MS12-009) Microsoft Windows AfdPoll Elevation of Privilege (2645640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0148

Update Details

Recommendation is updated

13291 - (MS12-008) Microsoft Windows Keyboard Layout Use After Free (2660465)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0154

Update Details

Recommendation is updated

13293 - (MS12-009) Microsoft Windows Ancillary Function Driver Elevation of Privilege (2645640)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0149

Update Details

Recommendation is updated

13294 - (MS12-009) Vulnerabilities In Ancillary Function Driver Could Allow Elevation Of Privilege (2645640)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0148, CVE-2012-0149

Update Details

Recommendation is updated

13396 - (MS12-018) Microsoft Windows PostMessage Function Elevation of Privilege (2641653)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0157

Update Details

Recommendation is updated

13399 - (MS12-018) Vulnerability In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2641653)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0157

Update Details

Recommendation is updated

13626 - (MS12-034) Microsoft Windows Scrollbar Calculation Privilege Escalation (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1848

Update Details

Recommendation is updated

13627 - (MS12-034) Microsoft Windows Keyboard Layout Privilege Escalation (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0181

Update Details

Recommendation is updated

13628 - (MS12-034) Microsoft Windows And Messages Privilege Escalation (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0180

Update Details

Recommendation is updated

13751 - (MS12-041) Microsoft Windows Clipboard Format Atom Name Handling Privilege Escalation (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1866

Update Details

Recommendation is updated

13776 - (MS12-041) Microsoft Windows Font Resource Refcount Integer Overflow Privilege Escalation (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1867

Update Details

Recommendation is updated

13777 - (MS12-041) Microsoft Windows String Atom Class Name Handling Privilege Escalation I (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1864

Update Details

Recommendation is updated

13778 - (MS12-041) Microsoft Windows String Atom Class Name Handling Privilege Escalation II (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1865

Update Details

Recommendation is updated

13781 - (MS12-042) Microsoft Windows User Mode Scheduler Memory Corruption Privilege Escalation (2711167)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0217

Update Details

Recommendation is updated

13785 - (MS12-041) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1864, CVE-2012-1865, CVE-2012-1866, CVE-2012-1867, CVE-2012-1868

Update Details

Recommendation is updated

13859 - (MS12-047) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1890, CVE-2012-1893

Update Details

Recommendation is updated

13860 - (MS12-047) Microsoft Windows Keyboard Layout Privilege Escalation (2718523)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1890

Update Details

Recommendation is updated

13861 - (MS12-047) Microsoft Windows Win32k Incorrect Type Handling Privilege Escalation (2718523)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1893

Update Details

Recommendation is updated

14016 - (MS12-055) Microsoft Windows Win32K User After Free Privilege Escalation (2731847)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2527

Update Details

Recommendation is updated

14215 - (MS12-068) Microsoft Windows Integer Overflow Information Disclosure (2724197)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2529

Update Details

Recommendation is updated

14218 - (MS12-068) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2529

Update Details

Recommendation is updated

14375 - (MS12-075) Microsoft Windows Win32k Use AfterFree Privilege Escalation I (2761226)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2530

Update Details

Recommendation is updated

14376 - (MS12-075) Microsoft Windows Win32k Use After Free Privilege Escalation II (2761159)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2553

Update Details

Recommendation is updated

14562 - (MS13-005) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0008

Update Details

Recommendation is updated

14563 - (MS13-005) Microsoft Windows Privilege Escalation (2778930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0008

Update Details

Recommendation is updated

14690 - (MS13-019) Microsoft Windows CSRSS Reference Count Local Privilege Escalation (2790113)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0076

Update Details

Recommendation is updated

14716 - (MS13-017) Microsoft Windows Race Condition I Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1278

Update Details

Recommendation is updated

14717 - (MS13-017) Microsoft Windows Race Condition II Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1279

Update Details

Recommendation is updated

14718 - (MS13-017) Microsoft Windows Reference Count Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1280

Update Details

Recommendation is updated

14822 - (MS13-023) Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2801261)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0079

Update Details

Recommendation is updated

14827 - (MS13-023) Microsoft Visio Viewer Tree Object Type Confusion Remote Code Execution (2801261)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0079

Update Details

Recommendation is updated

14930 - (MS13-036) Microsoft Windows Kernel OpenType Font Parsing Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1291

Update Details

Recommendation is updated

15069 - (MS13-046) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2840221)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1332, CVE-2013-1333, CVE-2013-1334

Update Details

Recommendation is updated

15070 - (MS13-046) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2840221)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1332

Update Details

Recommendation is updated

15071 - (MS13-046) Microsoft Windows Win32k Buffer Overflow Privilege Escalation (2840221)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1333

Update Details

Recommendation is updated

15072 - (MS13-046) Microsoft Windows Win32k Window Handle Privilege Escalation (2840221)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1334

Update Details

Recommendation is updated

15281 - (MS13-053) Microsoft Windows Kernel Read AV Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3660

Update Details

Recommendation is updated

15365 - (MS13-063) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (2859537)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-2556, CVE-2013-3196, CVE-2013-3197, CVE-2013-3198

Update Details

Recommendation is updated

15576 - (MS13-076) Vulnerabilities In Kernel-Mode Drivers Could Allow Elevation Of Privilege (2876315)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1341, CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, CVE-2013-3865, CVE-2013-3866

Update Details

Recommendation is updated

15933 - (MS13-093) Microsoft Windows Ancillary Function Driver Information Disclosure (2875783)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3887

Update Details

Recommendation is updated

15934 - (MS13-093) Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3887

Update Details

Recommendation is updated

16014 - (MS13-096) Microsoft Graphics Component Memory Corruption Remote Code Execution (2908005)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3906

Update Details

Recommendation is updated

16023 - (MS13-097) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5047

Update Details

Recommendation is updated

16024 - (MS13-101) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3899, CVE-2013-3902, CVE-2013-3903, CVE-2013-3907, CVE-2013-5058

Update Details

Recommendation is updated

16207 - (MS14-003) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2913602)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0262

Update Details

Recommendation is updated

16400 - (MS14-015) Vulnerabilities in Windows Kernel Mode Driver Could Allow Elevation of Privilege (2930275)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0300, CVE-2014-0323

Update Details

Recommendation is updated

16401 - (MS14-015) Microsoft Windows Kernel Mode Driver Win32k Privilege Escalation Privilege (2930275)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0300

Update Details

Recommendation is updated

16600 - (MS14-023) Vulnerability in Microsoft Office Could Allow Remote Code Execution (2961037)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1756, CVE-2014-1808

Update Details

Recommendation is updated

16964 - (MS14-047) Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0316

Update Details

Recommendation is updated

16965 - (MS14-047) Microsoft Windows ASLR Bypass Security Bypass (2978668)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0316

Update Details

Recommendation is updated

17228 - (MS14-058) Microsoft Windows Win32k.sys Privilege Escalation (3000061)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4113

Update Details

Recommendation is updated

17408 - (MS14-079) Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6317

Update Details

Recommendation is updated

17409 - (MS14-079) Microsoft Windows Kernel Denial of Service (3002885)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6317

Update Details

Recommendation is updated

17592 - (MS15-001) Vulnerability in Windows AppCompatCache could allow Elevation of Privilege (3023266)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0002

Update Details

Recommendation is updated

17593 - (MS15-001) Microsoft Windows Application Compatibility Infrastructure Privilege Escalation (3023266)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0002

Update Details

Recommendation is updated

17816 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0042

Update Details

Recommendation is updated

17817 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0043

Update Details

Recommendation is updated

17850 - (MS15-010) Microsoft Windows Win32k Privilege Escalation I (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0003

Update Details

Recommendation is updated

17851 - (MS15-010) Microsoft Windows CNG Feature Security Bypass (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0010

Update Details

Recommendation is updated

17852 - (MS15-010) Microsoft Windows Win32k Privilege Escalation II (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0057

Update Details

Recommendation is updated

17853 - (MS15-010) Microsoft Windows Cursor Object Double Free Privilege Escalation (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0058

Update Details

Recommendation is updated

17855 - (MS15-010) Microsoft Windows Font Driver Denial of Service (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0060

Update Details

Recommendation is updated

17857 - (MS15-010) Vulnerabilities in Windows Kernel Mode Driver Could Allow Remote Code Execution (3036220)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0003, CVE-2015-0010, CVE-2015-0057, CVE-2015-0058, CVE-2015-0059, CVE-2015-0060

Update Details

Recommendation is updated

18024 - (MS15-023) Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0077, CVE-2015-0078, CVE-2015-0094, CVE-2015-0095

Update Details

Recommendation is updated

18029 - (MS15-025) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0073, CVE-2015-0075

Update Details

Recommendation is updated

18151 - (MS15-038) Microsoft Windows NtCreateTransactionManager Type Confusion Privilege Escalation (3049576)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1643

Update Details

Recommendation is updated

18170 - (MS15-038) Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1643, CVE-2015-1644

Update Details

Recommendation is updated

18462 - (MS15-061) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1719, CVE-2015-1720, CVE-2015-1721, CVE-2015-1722, CVE-2015-1723, CVE-2015-1724, CVE-2015-1725, CVE-2015-1726, CVE-2015-1727, CVE-2015-1768, CVE-2015-2360

Update Details

Recommendation is updated

18464 - (MS15-061) Microsoft Windows Kernel Use-After-Free Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1720

Update Details

Recommendation is updated

18465 - (MS15-061) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1721

Update Details

Recommendation is updated

18467 - (MS15-061) Microsoft Windows Kernel Bitmap Handling Use-After-Free Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1722

Update Details

Recommendation is updated

18468 - (MS15-061) Microsoft Windows Station Use-After-Free Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1723

Update Details

Recommendation is updated

18470 - (MS15-061) Microsoft Windows Win32k Buffer Overflow Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1725

Update Details

Recommendation is updated

18474 - (MS15-061) Microsoft Windows Win32k Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2360

Update Details

Recommendation is updated

18565 - (HT204941) Apple iOS Multiple Vulnerabilities Prior To 8.4

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2013-1741, CVE-2014-8127, CVE-2014-8128, CVE-2014-8129, CVE-2014-8130, CVE-2015-1152, CVE-2015-1153, CVE-2015-1155, CVE-2015-1156, CVE-2015-1157, CVE-2015-3658, CVE-2015-3659, CVE-2015-3684, CVE-2015-3685, CVE-2015-3686, CVE-2015-3687, CVE-2015-3688, CVE-2015-3689, CVE-2015-3690, CVE-2015-3694, CVE-2015-3703, CVE-2015-3710, CVE-2015-3717, CVE-2015-3719, CVE-2015-3721, CVE-2015-3722, CVE-2015-3723, CVE-2015-3724, CVE-2015-3725, CVE-2015-3726, CVE-2015-3727, CVE-2015-3728, CVE-2015-4000, CVE-2015-7036

Update Details

CVE is updated

18589 - (MS15-073) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2363, CVE-2015-2365, CVE-2015-2366, CVE-2015-2367, CVE-2015-2381, CVE-2015-2382

Update Details

Recommendation is updated

18597 - (MS15-073) Microsoft Windows Kernel I Privilege Escalation (3070102)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2363

Update Details

Recommendation is updated

18598 - (MS15-073) Microsoft Windows Kernel II Privilege Escalation (3070102)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2365

Update Details

Recommendation is updated

18599 - (MS15-073) Microsoft Windows Kernel III Privilege Escalation (3070102)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2366

Update Details

Recommendation is updated

18603 - (MS15-076) Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2370

Update Details

Recommendation is updated

18604 - (MS15-076) Microsoft Windows DCOM RPC Privilege Escalation (3067505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2370

Update Details

Recommendation is updated

18799 - (MS15-085) Microsoft Windows Mount Manager Privilege Escalation (3082487)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1769

Update Details

Recommendation is updated

18806 - (MS15-085) Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1769

Update Details

Recommendation is updated

18903 - VideoLAN VLC Media Player 3GP File Arbitrary Pointer Dereference Vulnerability

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-5949

Update Details

Recommendation is updated

18952 - (MS15-102) Microsoft Windows Task Scheduler III Privilege Escalation (3089657)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2528

Update Details

Recommendation is updated

18953 - (MS15-102) Microsoft Windows Task Scheduler II Privilege Escalation (3089657)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2525

Update Details

Recommendation is updated

18954 - (MS15-102) Microsoft Windows Task Scheduler Privilege Escalation (3089657)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2524

Update Details

Recommendation is updated

18955 - (MS15-102) Vulnerability in Windows Task Management Could Allow Elevation of Privilege (3089657)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2524, CVE-2015-2525, CVE-2015-2528

Update Details

Recommendation is updated

18961 - (MS15-097) Microsoft Windows Graphics Font Driver I Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2507

Update Details

Recommendation is updated

18962 - (MS15-097) Microsoft Windows Graphics Font Driver II Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2508

Update Details

Recommendation is updated

18964 - (MS15-097) Microsoft Windows Graphics Memory Corruption I Remote Code Execution (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2511

Update Details

Recommendation is updated

18965 - (MS15-097) Microsoft Windows Graphics Memory Corruption II Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2512

Update Details

Recommendation is updated

18966 - (MS15-097) Microsoft Windows Graphics Memory Corruption III Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2517

Update Details

Recommendation is updated

18967 - (MS15-097) Microsoft Windows Graphics Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2518

Update Details

Recommendation is updated

18968 - (MS15-097) Microsoft Windows Graphics ASLR Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2527

Update Details

Recommendation is updated

18972 - (MS15-097) Microsoft Windows Graphics Memory Corruption IV Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2546

Update Details

Recommendation is updated

19098 - (MS15-111) Microsoft Windows Kernel Memory Corruption Privilege Escalation (3096447)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2549

Update Details

Recommendation is updated

19099 - (MS15-111) Microsoft Windows Elevation Privilege Escalation (3096447)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2550

Update Details

Recommendation is updated

19101 - (MS15-111) Microsoft Windows Mount Point Privilege Escalation (3096447)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2553

Update Details

Recommendation is updated

19102 - (MS15-111) Microsoft Windows Object Privilege Escalation (3096447)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2554

Update Details

Recommendation is updated

19104 - (MS15-111) Security Update for Windows Kernel to Address Elevation of Privilege (3096447)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2549, CVE-2015-2550, CVE-2015-2552, CVE-2015-2553, CVE-2015-2554

Update Details

Recommendation is updated

19215 - (MS15-119) Microsoft Windows Winsock Valid Memory Address Privilege Escalation (3104521)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2478

Update Details

Recommendation is updated Risk is updated

19217 - (MS15-119) Security Update in Winsock to Address Elevation of Privilege (3104521)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2478

Update Details

Recommendation is updated Risk is updated

19224 - (MS15-115) Microsoft Windows Kernel Privilege Escalation I (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6100

Update Details

Recommendation is updated Risk is updated

19225 - (MS15-115) Microsoft Windows Kernel Privilege Escalation II (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6101

Update Details

Recommendation is updated Risk is updated

19231 - (MS15-117) Security Update for NDIS to Address Elevation of Privilege (3101722)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6098

Update Details

Recommendation is updated Risk is updated

19232 - (MS15-117) Microsoft Windows NDIS Buffer Length Privilege Escalation (3101722)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6098

Update Details

Recommendation is updated Risk is updated

6164 - (MS08-064) Microsoft Virtual Address Descriptor Elevation of Privilege Vulnerability (956841)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4036

Update Details

Recommendation is updated

6169 - (MS08-061) Microsoft Windows Kernel Window Creation Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2250

Update Details

Recommendation is updated

6170 - (MS08-061) Microsoft Windows Kernel Unhandled Exception Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2251

Update Details

Recommendation is updated

6171 - (MS08-061) Microsoft Windows Kernel Memory Corruption Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2252

Update Details

Recommendation is updated

6493 - (MS09-006) Windows Kernel Handle Validation Vulnerability (958690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0082

Update Details

Recommendation is updated

6494 - (MS09-006) Windows Kernel Invalid Pointer Vulnerability (958690)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0083

Update Details

Recommendation is updated

6766 - (MS09-025) Microsoft Windows Desktop Parameter Edit Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1126

Update Details

Recommendation is updated

6767 - (MS09-025) Microsoft Windows Driver Class Registration Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1125

Update Details

Recommendation is updated

6768 - (MS09-025) Microsoft Windows Kernel Desktop Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1123

Update Details

Recommendation is updated

6769 - (MS09-025) Microsoft Windows Kernel Pointer Validation Vulnerability (968537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1124

Update Details

Recommendation is updated

7203 - (MS09-058) Windows Kernel Integer Underflow Vulnerability (971486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2515

Update Details

Recommendation is updated

7204 - (MS09-058) Windows Kernel NULL Pointer Dereference Vulnerability (971486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2516

Update Details

Recommendation is updated

7205 - (MS09-059) Local Security Authority Subsystem Service Integer Overflow Vulnerability (975467)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2524

Update Details

Recommendation is updated

7231 - (MS09-059) Vulnerability In Local Security Authority Subsystem Service Could Allow Denial Of Service (975467)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2524

Update Details

Recommendation is updated

7342 - Microsoft Windows SMB_PACKET Remote Kernel Denial-of-Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3676

Update Details

Recommendation is updated

7544 - (MS09-025) Vulnerabilities In Windows Kernel Could Allow Elevation of Privilege (968537)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1123, CVE-2009-1124, CVE-2009-1125, CVE-2009-1126

Update Details

Recommendation is updated

8054 - (MS08-064) Vulnerability In Virtual Address Descriptor Manipulation Could Allow Elevation Of Privilege (956841)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4036

Update Details

Recommendation is updated

8521 - (MS10-021) Microsoft Windows Kernel Memory Allocation Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0236

Update Details

Recommendation is updated

8522 - (MS10-021) Microsoft Windows Kernel Symbolic Link Creation Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0237

Update Details

Recommendation is updated

9073 - (MS10-032) Microsoft Windows Win32k Improper Data Validation Vulnerability (979559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0484

Update Details

Recommendation is updated

9074 - (MS10-032) Microsoft Windows Win32k Window Creation Vulnerability (979559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0485

Update Details

Recommendation is updated

9075 - (MS10-032) Microsoft Windows Win32k TrueType Font Parsing Vulnerability (979559)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1255

Update Details

Recommendation is updated

9679 - (MS10-058) Microsoft Windows Integer Overflow in Windows Networking Privilege Escalation (978886)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1893

Update Details

Recommendation is updated

9682 - (MS10-047) Microsoft Windows Kernel Improper Validation Denial Of Service (981852)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1890

Update Details

Recommendation is updated

9683 - (MS10-047) Microsoft Windows Kernel Double Free Privilege Escalation (981852)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1889

Update Details

Recommendation is updated

9684 - (MS10-047) Microsoft Windows Kernel Data Initialization Privilege Escalation (981852)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1888

Update Details

Recommendation is updated

10104 - (MS10-070) Microsoft ASP.NET AES Decrypt Security Bypass (2416728)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3332

Update Details

Recommendation is updated

10168 - (MS10-070) Microsoft ASP.NET AES Decrypt Security Bypass (2416728)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2010-3332

Update Details

Recommendation is updated

10358 - (MS10-073) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2549, CVE-2010-2743, CVE-2010-2744

Update Details

Recommendation is updated

10360 - (MS10-073) Microsoft Windows Win32K Reference Count Privilege Escalation (981957)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2549

Update Details

Recommendation is updated

10361 - (MS10-073) Microsoft Windows Win32K Keyboard Layout Privilege Escalation (981957)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2743

Update Details

Recommendation is updated

10362 - (MS10-073) Microsoft Windows Win32k Window Class Privilege Escalation (981957)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2744

Update Details

Recommendation is updated

16046 - (MS13-100) Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (2904244)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5059

Update Details

Recommendation is updated

16402 - (MS14-015) Microsoft Windows Kernel Mode Driver Win32k Information Disclosure (2930275)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0323

Update Details

Recommendation is updated

16496 - (MS14-019) Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2922229)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0315

Update Details

Recommendation is updated

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

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

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

17835 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-8967

Update Details

Recommendation is updated

17837 - (MS15-009) Cumulative Security Update for Internet Explorer (3034682)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-8967, CVE-2015-0017, CVE-2015-0018, CVE-2015-0019, CVE-2015-0020, CVE-2015-0021, CVE-2015-0022, CVE-2015-0023, CVE-2015-0025, CVE-2015-0026, CVE-2015-0027, CVE-2015-0028, CVE-2015-0029, CVE-2015-0030, CVE-2015-0031, CVE-2015-0035, CVE-2015-0036, CVE-2015-0037, CVE-2015-0038, CVE-2015-0039, CVE-2015-0040, CVE-2015-0041, CVE-2015-0042, CVE-2015-0043, CVE-2015-0044, CVE-2015-0045, CVE-2015-0046, CVE-2015-0048, CVE-2015-0049, CVE-2015-0050, CVE-2015-0051, CVE-2015-0052, CVE-2015-0053, CVE-2015-0054, CVE-2015-0055, CVE-2015-0066, CVE-2015-0067, CVE-2015-0068, CVE-2015-0069, CVE-2015-0070, CVE-2015-0071

Update Details

Recommendation is updated

17844 - (MS15-015) Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (3031432)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0062

Update Details

Recommendation is updated

18287 - (MS15-043) Microsoft Internet Explorer Privilege Escalation I (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1688

Update Details

Recommendation is updated

18293 - (MS15-043) Microsoft Internet Explorer Privilege Escalation II (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1703

Update Details

Recommendation is updated

18294 - (MS15-043) Microsoft Internet Explorer Privilege Escalation III (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1704

Update Details

Recommendation is updated

18303 - (MS15-043) Microsoft Internet Explorer Privilege Escalation IV (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1713

Update Details

Recommendation is updated

18435 - (MS15-056) Microsoft Internet Explorer Permissions III Privilege Escalation (3058515)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1748

Update Details

Recommendation is updated

18439 - (MS15-056) Microsoft Internet Explorer Permissions II Privilege Escalation (3058515)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1743

Update Details

Recommendation is updated

18443 - (MS15-056) Microsoft Internet Explorer Permissions I Privilege Escalation (3058515)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1739

Update Details

Recommendation is updated

18461 - (MS15-063) Microsoft Windows LoadLibrary Privilege Escalation (3063858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1758

Update Details

Recommendation is updated

18477 - (MS15-063) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1758

Update Details

Recommendation is updated

18610 - (MS15-070) Microsoft Excel DLL Remote Code Execution (3072620)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2378

Update Details

Recommendation is updated

18931 - (MS15-094) Microsoft Internet Explorer File Flags Tampering Privilege Escalation (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2484

Update Details

Recommendation is updated

19084 - (MS15-106) Microsoft Internet Explorer I Privilege Escalation (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6044

Update Details

Recommendation is updated

19088 - (MS15-106) Microsoft Internet Explorer II Privilege Escalation (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6047

Update Details

Recommendation is updated

19100 - (MS15-111) Microsoft Windows Trusted Boot Security Bypass (3096447)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2552

Update Details

Recommendation is updated

19237 - (MS15-120) Security Update for IPSec to Address Denial of Service (3102939)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6111

Update Details

Recommendation is updated

19238 - (MS15-120) Microsoft Windows IPSec Encryption Negotiation Denial of Service (3102939)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6111

Update Details

Recommendation is updated Risk is updated

130310 - Debian Linux 8.0 DSA-3391-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-7984

Update Details

Risk is updated CVE is updated

7202 - (MS09-058) Windows Kernel Exception Handler Vulnerability (971486)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2517

Update Details

Recommendation is updated

8519 - (MS10-021) Microsoft Windows Kernel Null Pointer Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0234

Update Details

Recommendation is updated

8520 - (MS10-021) Microsoft Windows Kernel Symbolic Link Value Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0235

Update Details

Recommendation is updated

8523 - (MS10-021) Microsoft Windows Kernel Registry Key Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0238

Update Details

Recommendation is updated

8524 - (MS10-021) Microsoft Windows Virtual Path Parsing Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0481

Update Details

Recommendation is updated

8525 - (MS10-021) Microsoft Windows Kernel Malformed Image Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0482

Update Details

Recommendation is updated

8526 - (MS10-021) Microsoft Windows Kernel Exception Handler Vulnerability (979683)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0810

Update Details

Recommendation is updated

9063 - (MS10-032) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (979559)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0484, CVE-2010-0485, CVE-2010-1255

Update Details

Recommendation is updated

9067 - (MS10-039) Vulnerabilities In Microsoft SharePoint Could Allow Elevation Of Privilege (2028554)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0817, CVE-2010-1257, CVE-2010-1264

Update Details

Recommendation is updated

9119 - (MS10-039) Microsoft SharePoint toStaticHTML Information Disclosure Vulnerability (2028554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1257

Update Details

Recommendation is updated

9763 - (MS10-049) Microsoft Windows TLS/SSL Renegotiation Vulnerability (980436)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3555

Update Details

Recommendation is updated

10199 - (MS10-070) Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-3332

Update Details

Recommendation is updated

11225 - (MS11-013) Microsoft Kerberos Spoofing (2496930)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0091

Update Details

Recommendation is updated

11770 - (MS11-034) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0662, CVE-2011-0665, CVE-2011-0666, CVE-2011-0667, CVE-2011-0670, CVE-2011-0671, CVE-2011-0672, CVE-2011-0673, CVE-2011-0674, CVE-2011-0676, CVE-2011-0677, CVE-2011-1225, CVE-2011-1226, CVE-2011-1227, CVE-2011-1228, CVE-2011-1229, CVE-2011-1230, CVE-2011-1231, CVE-2011-1232, CVE-2011-1233, CVE-2011-1234, CVE-2011-1235, CVE-2011-1236, CVE-2011-1237, CVE-2011-1238, CVE-2011-1239, CVE-2011-1240, CVE-2011-1241, CVE-2011-1242

Update Details

Recommendation is updated

12472 - (MS11-068) Microsoft Kernel Metadata Parsing Could Allow Denial of Service (2556532)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1971

Update Details

Recommendation is updated

12475 - (MS11-068) Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1971

Update Details

Recommendation is updated

12628 - (MS11-074) Microsoft XSS in SharePoint Calendar Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0653

Update Details

Recommendation is updated

12629 - (MS11-074) Microsoft SharePoint HTML Sanitization Information Disclosure (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1252

Update Details

Recommendation is updated

12630 - (MS11-074) Microsoft SharePoint Editform Script Injection Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1890

Update Details

Recommendation is updated

12631 - (MS11-074) Microsoft SharePoint Contact Details Reflected XSS Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1891

Update Details

Recommendation is updated

12632 - (MS11-074) Microsoft SharePoint Remote File Disclosure Information Disclosure (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1892

Update Details

Recommendation is updated

12633 - (MS11-074) Microsoft SharePoint XSS Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1893

Update Details

Recommendation is updated

12634 - (MS11-074) Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0653, CVE-2011-1252, CVE-2011-1890, CVE-2011-1891, CVE-2011-1892, CVE-2011-1893

Update Details

Recommendation is updated

12739 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k TrueType Font Type Translation (2567053)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-2002

Update Details

Recommendation is updated

13160 - (MS11-100) Microsoft .NET Form Authentication Spoofing (2638420)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-3415

Update Details

Recommendation is updated

13623 - (MS12-034) Microsoft Windows .NET Index Comparison Remote Code Execution (2681578)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0164

Update Details

Recommendation is updated

13779 - (MS12-041) Microsoft Windows Win32k.sys Race Condition Privilege Escalation (2709162)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1868

Update Details

Recommendation is updated

13783 - (MS12-039) Microsoft Windows HTML Sanitization Information Disclosure (2707956)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

Update Details

Recommendation is updated

13864 - (MS12-050) Microsoft SharePoint HTML Sanitization Information Disclosure (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

Update Details

Recommendation is updated

13865 - (MS12-050) Microsoft SharePoint Scriptresx.ashx Cross Site Scripting Privilege Escalation (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1859

Update Details

Recommendation is updated

13866 - (MS12-050) Microsoft SharePoint Search Scope Information Disclosure (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1860

Update Details

Recommendation is updated

13867 - (MS12-050) Microsoft SharePoint Script In Username Privilege Escalation (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1861

Update Details

Recommendation is updated

13868 - (MS12-050) Microsoft SharePoint URL Redirection Information Disclosure (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1862

Update Details

Recommendation is updated

13869 - (MS12-050) Microsoft SharePoint Reflected List Parameter Privilege Escalation (2695502)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1863

Update Details

Recommendation is updated

13870 - (MS12-050) Vulnerabilities In Microsoft SharePoint Could Allow Elevation Of Privilege (2695502)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858, CVE-2012-1859, CVE-2012-1860, CVE-2012-1861, CVE-2012-1862, CVE-2012-1863

Update Details

Recommendation is updated

13874 - (MS12-049) Microsoft Windows TLS Protocol Information Disclosure (2655992)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1870

Update Details

Recommendation is updated

13876 - (MS12-049) Vulnerability in TLS Could Allow Information Disclosure (2655992)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1870

Update Details

Recommendation is updated

14206 - (MS12-066) Microsoft Office HTML Sanitization Privilege Escalation (2741517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2520

Update Details

Recommendation is updated

14216 - (MS12-069) Microsoft Kerberos NULL Dereference Denial Of Service (2754673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2551

Update Details

Recommendation is updated

14217 - (MS12-069) Vulnerability in Kerberos Could Allow Denial of Service (2743555)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2551

Update Details

Recommendation is updated

14577 - (MS13-006) Microsoft Windows SSL And TLS Protocol Security Bypass (2785220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0013

Update Details

Recommendation is updated

14580 - (MS13-006) Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0013

Update Details

Recommendation is updated

14675 - (MS13-016) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2778344)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1248, CVE-2013-1249, CVE-2013-1250, CVE-2013-1251, CVE-2013-1252, CVE-2013-1253, CVE-2013-1254, CVE-2013-1255, CVE-2013-1256, CVE-2013-1257, CVE-2013-1258, CVE-2013-1259, CVE-2013-1260, CVE-2013-1261, CVE-2013-1262, CVE-2013-1263, CVE-2013-1264, CVE-2013-1265, CVE-2013-1266, CVE-2013-1267, CVE-2013-1268, CVE-2013-1269, CVE-2013-1270, CVE-2013-1271, CVE-2013-1272, CVE-2013-1273, CVE-2013-1274, CVE-2013-1275, CVE-2013-1276, CVE-2013-1277

Update Details

Recommendation is updated

14680 - (MS13-016) Microsoft Windows Race Condition I Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1248

Update Details

Recommendation is updated

14681 - (MS13-016) Microsoft Windows Race Condition II Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1249

Update Details

Recommendation is updated

14682 - (MS13-016) Microsoft Windows Race Condition III Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1250

Update Details

Recommendation is updated

14683 - (MS13-016) Microsoft Windows Race Condition IV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1251

Update Details

Recommendation is updated

14685 - (MS13-016) Microsoft Windows Race Condition IX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1256

Update Details

Recommendation is updated

14686 - (MS13-016) Microsoft Windows Race Condition V Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1252

Update Details

Recommendation is updated

14687 - (MS13-016) Microsoft Windows Race Condition VI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1253

Update Details

Recommendation is updated

14689 - (MS13-016) Microsoft Windows Race Condition VII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1254

Update Details

Recommendation is updated

14691 - (MS13-016) Microsoft Windows Race Condition XXX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1277

Update Details

Recommendation is updated

14692 - (MS13-016) Microsoft Windows Race Condition XXVIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1275

Update Details

Recommendation is updated

14694 - (MS13-016) Microsoft Windows Race Condition XXVII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1274

Update Details

Recommendation is updated

14705 - (MS13-009) Microsoft Internet Explorer Shift JIS Character Encoding Information Disclosure (2792100)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0015

Update Details

Recommendation is updated

14708 - (MS13-016) Microsoft Windows Race Condition VIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1255

Update Details

Recommendation is updated

14709 - (MS13-016) Microsoft Windows Race Condition X Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1257

Update Details

Recommendation is updated

14710 - (MS13-016) Microsoft Windows Race Condition XI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1258

Update Details

Recommendation is updated

14720 - (MS13-016) Microsoft Windows Race Condition XII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1259

Update Details

Recommendation is updated

14721 - (MS13-016) Microsoft Windows Race Condition XIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1260

Update Details

Recommendation is updated

14722 - (MS13-016) Microsoft Windows Race Condition XIV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1261

Update Details

Recommendation is updated

14723 - (MS13-016) Microsoft Windows Race Condition XIX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1266

Update Details

Recommendation is updated

14724 - (MS13-016) Microsoft Windows Race Condition XV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1262

Update Details

Recommendation is updated

14725 - (MS13-016) Microsoft Windows Race Condition XVI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1263

Update Details

Recommendation is updated

14726 - (MS13-016) Microsoft Windows Race Condition XVII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1264

Update Details

Recommendation is updated

14727 - (MS13-016) Microsoft Windows Race Condition XVIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1265

Update Details

Recommendation is updated

14728 - (MS13-016) Microsoft Windows Race Condition XX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1267

Update Details

Recommendation is updated

14729 - (MS13-016) Microsoft Windows Race Condition XXI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1268

Update Details

Recommendation is updated

14730 - (MS13-016) Microsoft Windows Race Condition XXII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1269

Update Details

Recommendation is updated

14731 - (MS13-016) Microsoft Windows Race Condition XXIII Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1270

Update Details

Recommendation is updated

14732 - (MS13-016) Microsoft Windows Race Condition XXIV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1271

Update Details

Recommendation is updated

14733 - (MS13-016) Microsoft Windows Race Condition XXIX Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1276

Update Details

Recommendation is updated

14734 - (MS13-016) Microsoft Windows Race Condition XXV Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1272

Update Details

Recommendation is updated

14736 - (MS13-016) Microsoft Windows Race Condition XXVI Privilege Escalation (2778344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1273

Update Details

Recommendation is updated

14824 - (MS13-025) Vulnerability in Microsoft OneNote Could Allow Information Disclosure (2816264)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0086

Update Details

Recommendation is updated

14842 - (MS13-025) Microsoft OneNote Buffer Size Validation Information Disclosure (2816264)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0086

Update Details

Recommendation is updated

14929 - (MS13-036) Microsoft Windows Kernel Race Condition I Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1283

Update Details

Recommendation is updated

14931 - (MS13-036) Microsoft Windows Kernel Race Condition II Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1292

Update Details

Recommendation is updated

14932 - (MS13-036) Microsoft Windows Kernel NTFS Pointer Dereference Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1293

Update Details

Recommendation is updated

14933 - (MS13-031) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1284, CVE-2013-1294

Update Details

Recommendation is updated

14935 - (MS13-031) Microsoft Windows Kernel Race Condition I Privilege Escalation (2813170)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1284

Update Details

Recommendation is updated

14936 - (MS13-031) Microsoft Windows Kernel Race Condition II Privilege Escalation (2813170)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1294

Update Details

Recommendation is updated

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

15035 - (MS13-044) Vulnerability In Microsoft Visio Could Allow Information Disclosure (2834692)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1301

Update Details

Recommendation is updated

15036 - (MS13-044) Microsoft Office Visio XML External Entities Resolution Information Disclosure (2834692)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1301

Update Details

Recommendation is updated

15182 - (MS13-048) Microsoft Windows Kernel Information Disclosure (2839229)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3136

Update Details

Recommendation is updated

15183 - (MS13-048) Vulnerability in Windows Kernel Could Allow Information Disclosure (2839229)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3136

Update Details

Recommendation is updated

15257 - (MS13-053) Microsoft Windows Kernel Buffer Overflow Remote Code Execution (2850851)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3172

Update Details

Recommendation is updated

15371 - (MS13-063) Microsoft Windows Kernel Memory Corruption III Remote Code Execution (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3198

Update Details

Recommendation is updated

15372 - (MS13-063) Microsoft Windows Kernel Memory Corruption II Remote Code Execution (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3197

Update Details

Recommendation is updated

15373 - (MS13-063) Microsoft Windows Kernel Memory Corruption I Remote Code Execution (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3196

Update Details

Recommendation is updated

15374 - (MS13-063) Microsoft Windows Kernel ASLR Security Bypass (2859537)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-2556

Update Details

Recommendation is updated

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

15575 - (MS13-075) Vulnerability In Microsoft Office IME (Chinese) Could Allow Elevation Of Privilege (2878687)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3859

Update Details

Recommendation is updated

15577 - (MS13-075) Microsoft Office Chinese IME Privilege Escalation (2878687)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3859

Update Details

Recommendation is updated

15579 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation I (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1341

Update Details

Recommendation is updated

15580 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation II (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1342

Update Details

Recommendation is updated

15581 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation III (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1343

Update Details

Recommendation is updated

15582 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation IV (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1344

Update Details

Recommendation is updated

15583 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation V (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3864

Update Details

Recommendation is updated

15584 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation VI (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3865

Update Details

Recommendation is updated

15585 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation VII (2876315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3866

Update Details

Recommendation is updated

15587 - (MS13-077) Microsoft Windows Service Control Manager Double Free Privilege Escalation (2872339)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3862

Update Details

Recommendation is updated

15589 - (MS13-077) Microsoft Windows Service Control Manager Double Free Privilege Escalation (2872339)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3862

Update Details

Recommendation is updated

15590 - (MS13-073) Microsoft Office Memory Corruption Remote Code Execution II (2858300)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3158

Update Details

Recommendation is updated

15592 - (MS13-073) Microsoft Office XML External Entities Resolution Information Disclosure (2858300)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3159

Update Details

Recommendation is updated

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

15735 - (MS13-081) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3888

Update Details

Recommendation is updated

15736 - (MS13-081) Microsoft Windows Win32k NULL Page Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3881

Update Details

Recommendation is updated

15737 - (MS13-081) Microsoft Windows App Container Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3880

Update Details

Recommendation is updated

15738 - (MS13-081) Microsoft Windows Win32k Use After Free Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE 2013-3879

Update Details

Recommendation is updated

15739 - (MS13-081) Microsoft Windows USB Descriptor Privilege Escalation (2870008)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3200

Update Details

Recommendation is updated

15917 - (MS13-088) Microsoft Internet Explorer CSS Characters Information Disclosure (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3909

Update Details

Recommendation is updated

15918 - (MS13-088) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3910

Update Details

Recommendation is updated

15919 - (MS13-088) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3911

Update Details

Recommendation is updated

15920 - (MS13-088) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3912

Update Details

Recommendation is updated

15921 - (MS13-088) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3914

Update Details

Recommendation is updated

15922 - (MS13-088) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3915

Update Details

Recommendation is updated

15923 - (MS13-088) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3916

Update Details

Recommendation is updated

15924 - (MS13-088) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3917

Update Details

Recommendation is updated

15925 - (MS13-088) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3871

Update Details

Recommendation is updated

15926 - (MS13-088) Microsoft Internet Explorer Print Preview Information Disclosure (2888505)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3908

Update Details

Recommendation is updated

15929 - (MS13-091) Microsoft Office Word Buffer Overflow Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1324

Update Details

Recommendation is updated

15930 - (MS13-091) Microsoft Office Word Heap Overwrite Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1325

Update Details

Recommendation is updated

15931 - (MS13-091) Microsoft Office WPD File Format Remote Code Execution (2885093)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0082

Update Details

Recommendation is updated

16021 - (MS13-097) Microsoft Internet Explorer Memory Corruption I Privilege Escalation (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5045

Update Details

Recommendation is updated

16022 - (MS13-097) Microsoft Internet Explorer Memory Corruption II Privilege Escalation (2898785)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5046

Update Details

Recommendation is updated

16025 - (MS13-104) Vulnerability in Microsoft Office Could Allow Information Disclosure (2909976)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5054

Update Details

Recommendation is updated

16033 - (MS13-101) Microsoft Windows Integer Overflow I Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3899

Update Details

Recommendation is updated

16034 - (MS13-101) Microsoft Windows Use-After-Free Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3902

Update Details

Recommendation is updated

16035 - (MS13-101) Microsoft Windows TrueType Font Parsing Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3903

Update Details

Recommendation is updated

16036 - (MS13-101) Microsoft Windows Port-Class Driver Double Fetch Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3907

Update Details

Recommendation is updated

16037 - (MS13-101) Microsoft Windows Integer Overflow II Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5058

Update Details

Recommendation is updated

16038 - (MS13-104) Microsoft Office Token Hijacking Information Disclosure (2909976)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5054

Update Details

Recommendation is updated

16208 - (MS14-003) Microsoft Windows Kernel-Mode Drivers Privilege Elevation (2913602)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0262

Update Details

Recommendation is updated

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

16491 - (MS14-020) Microsoft Publisher Pointer Dereference Remote Code Execution (2950145)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1759

Update Details

Recommendation is updated

16497 - (MS14-019) Microsoft Windows File Handling Remote Code Execution (2922229)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0315

Update Details

Recommendation is updated

16603 - (MS14-023) Microsoft Office Chinese Grammar Checking Remote Code Execution (2961037)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1756

Update Details

Recommendation is updated

16605 - (MS14-023) Microsoft Office Token Reuse Remote Code Execution (2961037)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1808

Update Details

Recommendation is updated

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

16846 - (MS14-040) Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2975684)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1767

Update Details

Recommendation is updated

16872 - (MS14-040) Microsoft Windows Ancillary Function Driver Privilege Escalation (2975684)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1767

Update Details

Recommendation is updated

17057 - Drupal Multiple Denial of Service Vulnerabilities

Category: General Vulnerability Assessment -> Instrusive -> Web Server

Risk Level: Medium

CVE: CVE-2014-5265, CVE-2014-5266, CVE-2014-5267

Update Details

FASLScript 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

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

17824 - (MS15-009) Microsoft Internet Explorer ASLR Security Bypass I (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0051

Update Details

Recommendation is updated

17827 - (MS15-009) Microsoft Internet Explorer Privilege Escalation I (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0054

Update Details

Recommendation is updated

17828 - (MS15-009) Microsoft Internet Explorer Privilege Escalation II (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0055

Update Details

Recommendation is updated

17832 - (MS15-009) Microsoft Internet Explorer ASLR Security Bypass II (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0069

Update Details

Recommendation is updated

17833 - (MS15-009) Microsoft Internet Explorer Cross-Domain Information Disclosure (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0070

Update Details

Recommendation is updated

17834 - (MS15-009) Microsoft Internet Explorer ASLR Security Bypass III (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0071

Update Details

Recommendation is updated

17842 - (MS15-015) Microsoft Windows Create Process Privilege Escalation (3031432)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0062

Update Details

Recommendation is updated

17984 - (MS15-022) Microsoft Office Sharepoint Cross-Site Scripting Privilege Escalation II (3038999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1636

Update Details

Recommendation is updated

17985 - (MS15-022) Microsoft Office Sharepoint Cross-Site Scripting Privilege Escalation I (3038999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1633

Update Details

Recommendation is updated

17986 - (MS15-022) Microsoft Office World Local Zone Remote Code Execution (3038999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0097

Update Details

Recommendation is updated

17988 - (MS15-022) Microsoft Office Memory Handling Remote Code Execution (3038999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0085

Update Details

Recommendation is updated

18012 - (MS15-018) Microsoft Internet Explorer Memory Corruption I Privilege Escalation (3032359)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0072

Update Details

Recommendation is updated

18014 - (MS15-018) Microsoft Internet Explorer Memory Corruption II Privilege Escalation (3032359)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1627

Update Details

Recommendation is updated

18025 - (MS15-023) Microsoft Windows Kernel Calling Thread Privilege Escalation (3034344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0078

Update Details

Recommendation is updated

18026 - (MS15-023) Microsoft Windows Kernel Memory I Information Disclosure (3034344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0077

Update Details

Recommendation is updated

18027 - (MS15-023) Microsoft Windows Kernel Memory II Information Disclosure (3034344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0094

Update Details

Recommendation is updated

18028 - (MS15-023) Microsoft Windows Kernel Memory III Information Disclosure (3034344)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0095

Update Details

Recommendation is updated

18030 - (MS15-025) Microsoft Office Kernel Impersonation Level Check Privilege Escalation (3038680)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0075

Update Details

Recommendation is updated

18031 - (MS15-025) Microsoft Windows Registry Virtualization Privilege Escalation (3038680)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0073

Update Details

Recommendation is updated

18041 - (MS15-031) Vulnerability in Schannel Could Allow Security Feature Bypass (3046015)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1637

Update Details

Recommendation is updated

18043 - (MS15-031) Microsoft Windows Schannel Security Bypass (3046049)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1637

Update Details

Recommendation is updated

18142 - (MS15-032) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3038314)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1661

Update Details

Recommendation is updated

18171 - (MS15-038) Microsoft Windows MS-DOS Device Name Privilege Escalation (3049576)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1644

Update Details

Recommendation is updated

18187 - (MS15-033) Microsoft Outlook Mac App Cross-Site Scripting (3048019)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-1639

Update Details

Recommendation is updated

18265 - (MS15-046) Microsoft Office Memory Corruption I Remote Code Execution (3057181)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1682

Update Details

Recommendation is updated

18267 - (MS15-046) Microsoft Office Memory Corruption I Remote Code Execution (3057181)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-1682

Update Details

Recommendation is updated

18278 - (MS15-055) Microsoft Windows Schannel Information Disclosure (3061518)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1716

Update Details

Recommendation is updated

18305 - (MS15-044) Microsoft Windows GDI+ OpenType Font Parsing Remote Code Execution (3057110)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1670

Update Details

Recommendation is updated

18311 - (MS15-055) Vulnerability in Schannel Could Allow Information Disclosure (3061518)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1716

Update Details

Recommendation is updated

18469 - (MS15-061) Microsoft Windows Kernel Object Use-After-Free Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1724

Update Details

Recommendation is updated

18650 - (MS15-070) Microsoft Office Memory Corruption VI Remote Code Execution (3072620)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2424

Update Details

Recommendation is updated

18921 - (MS15-101) Microsoft .NET Framework MVC Denial of Service (3089662)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2526

Update Details

Recommendation is updated

18932 - (MS15-094) Microsoft Internet Explorer Memory Handling I Information Disclosure (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2483

Update Details

Recommendation is updated

19072 - (MS15-107) Microsoft Edge Memory Information Disclosure I (3096448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6057

Update Details

Recommendation is updated

19075 - (MS15-107) Cumulative Security Update for Microsoft Edge (3096448)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6057, CVE-2015-6058

Update Details

Recommendation is updated

19094 - (MS15-106) Microsoft Internet Explorer III Information Disclosure (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6053

Update Details

Recommendation is updated

19268 - (MS15-121) Microsoft Windows Schannel Triple Handshake Spoofing Information Disclosure (3081320)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6112

Update Details

Recommendation is updated

19269 - (MS15-121) Security Update for Schannel to Address Spoofing (3081320)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6112

Update Details

Recommendation is updated Risk is updated

8708 - Microsoft Office SharePoint 'cid0' Cross-Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2010-0817

Update Details

Recommendation is updated

9083 - (MS10-039) Microsoft Office SharePoint 'cid0' Cross-Site Scripting Vulnerability (983438)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0817

Update Details

Recommendation is updated

9084 - (MS10-039) Microsoft Office Sharepoint Help Page Denial of Service Vulnerability (2028554)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1264

Update Details

Recommendation is updated

9697 - (MS10-048) Microsoft Windows Win32k Pool Overflow Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1887

Update Details

Recommendation is updated

9698 - (MS10-048) Microsoft Windows Win32k Bounds Checking Vulnerability (2160329)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1887

Update Details

Recommendation is updated

14205 - (MS12-066) Vulnerabilities in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2520

Update Details

Recommendation is updated

17224 - (MS14-057) Microsoft .NET Framework Address Space Layout Randomization Security Bypass (3000414)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4122

Update Details

Recommendation is updated

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

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

18284 - (MS15-043) Microsoft Internet Explorer VBScript ASLR Security Bypass I (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1684

Update Details

Recommendation is updated

18285 - (MS15-043) Microsoft Internet Explorer ASLR Security Bypass (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1685

Update Details

Recommendation is updated

18286 - (MS15-043) Microsoft Internet Explorer VBScript ASLR Security Bypass II (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1686

Update Details

Recommendation is updated

18291 - (MS15-043) Microsoft Internet Explorer Clipboard Information Disclosure (3049563)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1692

Update Details

Recommendation is updated

18428 - (MS15-056) Microsoft Internet Explorer History Information Disclosure (3058515)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1765

Update Details

Recommendation is updated

18609 - (MS15-070) Microsoft Excel ASLR Bypass Information Disclosure (3072620)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2375

Update Details

Recommendation is updated

18619 - (MS15-065) Microsoft Internet Explorer Information Disclosure I (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1729

Update Details

Recommendation is updated

18634 - (MS15-065) Microsoft Internet Explorer Filter Bypass Cross-Site Scripting I (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2398

Update Details

Recommendation is updated

18642 - (MS15-065) Microsoft Internet Explorer Information Disclosure III (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2410

Update Details

Recommendation is updated

18644 - (MS15-065) Microsoft Internet Explorer Information Disclosure IV (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2412

Update Details

Recommendation is updated

18645 - (MS15-065) Microsoft Internet Explorer Information Disclosure V (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2413

Update Details

Recommendation is updated

18646 - (MS15-065) Microsoft Internet Explorer Information Disclosure VI (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2414

Update Details

Recommendation is updated

18648 - (MS15-065) Microsoft Internet Explorer ASLR Security Bypass (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2421

Update Details

Recommendation is updated

18653 - (MS15-065) Microsoft Internet Explorer Information Disclosure II (3076321)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2402

Update Details

Recommendation is updated

18761 - (MS15-079) Microsoft Internet Explorer Unsafe Command Line Parameter Information Disclosure (3082442)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

Update Details

Recommendation is updated

18772 - (MS15-079) Microsoft Internet Explorer ASLR Security Bypass I (3082442)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2445

Update Details

Recommendation is updated

18773 - (MS15-079) Microsoft Internet Explorer ASLR Security Bypass II (3082442)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2449

Update Details

Recommendation is updated

18794 - (MS15-080) Microsoft Windows CSRSS Privilege Escalation (3078662)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2453

Update Details

Recommendation is updated

18804 - (MS15-091) Microsoft Edge ASLR Bypass Security Bypass (3084525)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2449

Update Details

Recommendation is updated

18817 - (MS15-088) Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

Update Details

Recommendation is updated

18823 - (MS15-081) Microsoft Office Command Line Parameter Unsafe Passing Information Disclosure (3080790)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

Update Details

Recommendation is updated

18830 - (MS15-088) Microsoft Windows Command Line Parameter Unsafe Passing Information Disclosure (3082458)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

Update Details

Recommendation is updated

18934 - (MS15-094) Microsoft Internet Explorer Permissions Privilege Escalation (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2489

Update Details

Recommendation is updated

18975 - (MS15-098) Microsoft Windows Journal Denial of Service (3089669)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2516

Update Details

Recommendation is updated

19074 - (MS15-107) Microsoft Edge Filter Cross-Site Scripting (3096448)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6058

Update Details

Recommendation is updated

19085 - (MS15-110) Microsoft SharePoint Information Disclosure (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2556

Update Details

Recommendation is updated

19087 - (MS15-106) Microsoft Internet Explorer II Information Disclosure (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6046

Update Details

Recommendation is updated

19092 - (MS15-106) Microsoft Internet Explorer III Privilege Escalation (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6051

Update Details

Recommendation is updated

19093 - (MS15-106) Microsoft Internet Explorer VBScript and Jscript ASLR Security Bypass (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6052

Update Details

Recommendation is updated

19097 - (MS15-106) Microsoft Internet Explorer Information Disclosure (3096441)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6059

Update Details

Recommendation is updated

19221 - (MS15-113) Microsoft Edge ASLR Security Bypass (3104519)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6088

Update Details

Recommendation is updated Risk is updated

19233 - (MS15-118) Security Updates in .NET Framework to Address Elevation of Privilege (3104507)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6096, CVE-2015-6099, CVE-2015-6115

Update Details

Recommendation is updated

19234 - (MS15-118) Microsoft .NET Framework ASLR Security Bypass (3104507)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6115

Update Details

Recommendation is updated Risk is updated

19235 - (MS15-118) Microsoft .NET Framework DTD Parsing Privilege Escalation I (3104507)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6096

Update Details

Recommendation is updated Risk is updated

19236 - (MS15-118) Microsoft .NET Framework HTTP Request Privilege Escalation II (3104507)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6099

Update Details

Recommendation is updated Risk is updated

19262 - (MS15-112) Microsoft Internet Explorer Information Disclosure (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6086

Update Details

Recommendation is updated Risk is updated

19264 - (MS15-112) Microsoft Internet Explorer ASLR Security Bypass (3104517)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6088

Update Details

Recommendation is updated Risk is updated

19270 - (MS15-122) Microsoft Windows Kerberos Password Change Security Bypass (3105256)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6095

Update Details

Recommendation is updated Risk is updated

19271 - (MS15-122) Security Update for Kerberos to Address Security Feature Bypass (3105256)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6095

Update Details

Recommendation is updated Risk is updated

19272 - (MS15-123) Microsoft Skype For Business Server Input Validation Information Disclosure (3105872)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6061

Update Details

Recommendation is updated Risk is updated

19273 - (MS15-123) Security Update for Skype for Business and Lync to Address Information Disclosure (3105872)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6061

Update Details

Recommendation is updated Risk is updated

189907 - Fedora Linux 23 FEDORA-2015-b15b90eeaa Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-0856

Update Details

Risk is updated

189976 - Fedora Linux 22 FEDORA-2015-9f996ea146 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-0856

Update Details

Risk is updated

18945 - (MS15-099) Microsoft Office Sharepoint Cross Site Scripting Information Disclosure (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2522

Update Details

Recommendation is updated

19107 - (MS15-110) Microsoft Office Web Apps Spoofing Cross-Site Scripting (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6037

Update Details

Recommendation is updated

19108 - (MS15-110) Microsoft SharePoint Security Bypass (3089664)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6039

Update Details

Recommendation is updated

19230 - (MS15-115) Microsoft Windows Kernel Permissions Validation Security Bypass (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6113

Update Details

Recommendation is updated Risk is updated

32831 - Oracle Solaris 145334-34 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-2015-2616

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32838 - Oracle Solaris 145336-20 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32839 - Oracle Solaris 145333-34 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-2015-2616

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32842 - Oracle Solaris 145335-20 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33034 - Oracle Solaris 145646-08 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33035 - Oracle Solaris 145647-08 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

12336 - (MS11-054) Microsoft Windows Win32k Incorrect Parameter Privilege Escalation (2555917)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2011-1886

Update Details

Recommendation is updated

18463 - (MS15-061) Microsoft Windows Kernel Information Disclosure (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1719

Update Details

Recommendation is updated

18471 - (MS15-061) Microsoft Windows Kernel Brush Object Use-After-Free Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1726

Update Details

Recommendation is updated

18472 - (MS15-061) Microsoft Windows Win32k Pool Buffer Overflow Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1727

Update Details

Recommendation is updated

18473 - (MS15-061) Microsoft Windows Win32k Memory Corruption Privilege Escalation (3057839)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1768

Update Details

Recommendation is updated

18600 - (MS15-073) Microsoft Windows Kernel I Information Disclosure (3070102)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2367

Update Details

Recommendation is updated

18601 - (MS15-073) Microsoft Windows Kernel II Information Disclosure (3070102)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2381

Update Details

Recommendation is updated

18602 - (MS15-073) Microsoft Windows Kernel III Information Disclosure (3070102)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2382

Update Details

Recommendation is updated

18795 - (MS15-080) Microsoft Windows KMD Security Bypass (3078662)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2454

Update Details

Recommendation is updated

18796 - (MS15-080) Microsoft Windows Shell Security Bypass (3078662)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2465

Update Details

Recommendation is updated

18798 - (MS15-080) Microsoft Windows Kernel ASLR Security Bypass (3078662)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2433

Update Details

Recommendation is updated

18971 - (MS15-097) Microsoft Windows Graphics Security Bypass (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2529

Update Details

Recommendation is updated

19226 - (MS15-115) Microsoft Windows Kernel KASLR Information Disclosure I (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6102

Update Details

Recommendation is updated Risk is updated

19229 - (MS15-115) Microsoft Windows Kernel KASLR Information Disclosure II (3105864)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6109

Update Details

Recommendation is updated Risk is updated

18273 - (MS15-052) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1674

Update Details

Recommendation is updated

18299 - (MS15-052) Microsoft Windows Kernel Security Bypass (3050514)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1674

Update Details

Recommendation is updated

18926 - (MS15-105) Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass (3091287)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2534

Update Details

Recommendation is updated

18927 - (MS15-105) Microsoft Windows Hyper-V Security Bypass (3091287)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2534

Update Details

Recommendation is updated

70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70086 - oracle.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.