

MCAFFEE 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

141460 - Red Hat Enterprise Linux RHSA-2017-0217 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2847, CVE-2016-7117

Description

The scan detected that the host is missing the following update:
RHSA-2017-0217

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0217.html>

RHEL7_2S

noarch

kernel-abi-whitelists-3.10.0-327.46.1.el7

kernel-doc-3.10.0-327.46.1.el7

x86_64

kernel-tools-libs-devel-3.10.0-327.46.1.el7

python-perf-debuginfo-3.10.0-327.46.1.el7

kernel-devel-3.10.0-327.46.1.el7

kernel-debuginfo-3.10.0-327.46.1.el7

kernel-tools-libs-3.10.0-327.46.1.el7

kernel-debug-3.10.0-327.46.1.el7

kernel-3.10.0-327.46.1.el7

kernel-headers-3.10.0-327.46.1.el7

python-perf-3.10.0-327.46.1.el7

kernel-debug-devel-3.10.0-327.46.1.el7

perf-3.10.0-327.46.1.el7

kernel-tools-3.10.0-327.46.1.el7

kernel-debug-debuginfo-3.10.0-327.46.1.el7

kernel-debuginfo-common-x86_64-3.10.0-327.46.1.el7

kernel-tools-debuginfo-3.10.0-327.46.1.el7

perf-debuginfo-3.10.0-327.46.1.el7

141496 - Red Hat Enterprise Linux RHSA-2016-2073 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
RHSA-2016-2073

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2073.html>

RHEL6_7S

i386

openssl-static-1.0.1e-42.el6_7.5
openssl-devel-1.0.1e-42.el6_7.5
openssl-debuginfo-1.0.1e-42.el6_7.5
openssl-perl-1.0.1e-42.el6_7.5
openssl-1.0.1e-42.el6_7.5

x86_64

openssl-static-1.0.1e-42.el6_7.5
openssl-devel-1.0.1e-42.el6_7.5
openssl-debuginfo-1.0.1e-42.el6_7.5
openssl-perl-1.0.1e-42.el6_7.5
openssl-1.0.1e-42.el6_7.5

141503 - Red Hat Enterprise Linux RHSA-2015-1030 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1421

Description

The scan detected that the host is missing the following update:
RHSA-2015-1030

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-1030.html>

RHEL6_4S

i386

kernel-debug-devel-2.6.32-358.61.1.el6
kernel-debuginfo-common-i686-2.6.32-358.61.1.el6
perf-2.6.32-358.61.1.el6
python-perf-2.6.32-358.61.1.el6
kernel-headers-2.6.32-358.61.1.el6
kernel-debug-2.6.32-358.61.1.el6
perf-debuginfo-2.6.32-358.61.1.el6
kernel-2.6.32-358.61.1.el6
kernel-debug-debuginfo-2.6.32-358.61.1.el6
kernel-devel-2.6.32-358.61.1.el6
kernel-debuginfo-2.6.32-358.61.1.el6
python-perf-debuginfo-2.6.32-358.61.1.el6

noarch

kernel-firmware-2.6.32-358.61.1.el6
kernel-doc-2.6.32-358.61.1.el6

x86_64
kernel-debug-devel-2.6.32-358.61.1.el6
python-perf-2.6.32-358.61.1.el6
perf-2.6.32-358.61.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.61.1.el6
kernel-headers-2.6.32-358.61.1.el6
kernel-debug-2.6.32-358.61.1.el6
perf-debuginfo-2.6.32-358.61.1.el6
kernel-2.6.32-358.61.1.el6
kernel-debug-debuginfo-2.6.32-358.61.1.el6
kernel-devel-2.6.32-358.61.1.el6
kernel-debuginfo-2.6.32-358.61.1.el6
python-perf-debuginfo-2.6.32-358.61.1.el6

185618 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3227-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9911, CVE-2015-4844, CVE-2016-0494, CVE-2016-6293, CVE-2016-7415

Description

The scan detected that the host is missing the following update:
USN-3227-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003771.html>

Ubuntu 12.04

libicu48_4.8.1.1-3ubuntu0.7

Ubuntu 16.04

libicu55_55.1-7ubuntu0.1

Ubuntu 14.04

libicu52_52.1-3ubuntu0.5

Ubuntu 16.10

libicu57_57.1-4ubuntu0.1

21246 - (SB10187) McAfee ePolicy Orchestrator SQL Injection Vulnerability

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

Risk Level: High

CVE: CVE-2016-8027

Description

An SQL injection vulnerability is present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

An SQL injection vulnerability is present in some versions of McAfee ePolicy Orchestrator. A specially crafted HTTP post can allow an attacker to alter a SQL query. Successful exploitation could result in disclosure of information within the database or impersonation of an agent without authentication.

21512 - (MS16-148) Microsoft Office Memory Corruption Remote Code Execution IV (3204068)

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

Risk Level: High

CVE: CVE-2016-7274

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw occurs when the Office software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

141462 - Red Hat Enterprise Linux RHSA-2017-0459 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
RHSA-2017-0459

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0459.html>

RHEL5S

i386

firefox-45.8.0-2.el5_11

firefox-debuginfo-45.8.0-2.el5_11

x86_64

firefox-45.8.0-2.el5_11

firefox-debuginfo-45.8.0-2.el5_11

RHEL6D

x86_64

firefox-45.8.0-2.el6_8

firefox-debuginfo-45.8.0-2.el6_8

i386
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

RHEL6S
i386
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

x86_64
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

RHEL6WS
x86_64
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

i386
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

RHEL5D
x86_64
firefox-45.8.0-2.el5_11
firefox-debuginfo-45.8.0-2.el5_11

i386
firefox-45.8.0-2.el5_11
firefox-debuginfo-45.8.0-2.el5_11

141465 - Red Hat Enterprise Linux RHSA-2017-0461 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
RHSA-2017-0461

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0461.html>

RHEL7D
x86_64
firefox-debuginfo-52.0-4.el7_3
firefox-52.0-4.el7_3

RHEL7S
x86_64
firefox-debuginfo-52.0-4.el7_3
firefox-52.0-4.el7_3

RHEL7WS
x86_64
firefox-debuginfo-52.0-4.el7_3
firefox-52.0-4.el7_3

160222 - CentOS 5, 6 CESA-2017-0459 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
CESA-2017-0459

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022326.html>

<http://lists.centos.org/pipermail/centos-announce/2017-March/022327.html>

CentOS 5
x86_64
firefox-45.8.0-2.el5.centos

i386
firefox-45.8.0-2.el5.centos

CentOS 6
x86_64
firefox-45.8.0-2.el6.centos

i686
firefox-45.8.0-2.el6.centos

160223 - CentOS 7 CESA-2017-0461 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
CESA-2017-0461

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022334.html>

CentOS 7
x86_64

firefox-52.0-4.el7.centos

i686

firefox-52.0-4.el7.centos

163296 - Oracle Enterprise Linux ELSA-2017-0461 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
ELSA-2017-0461

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006777.html>

OEL7

x86_64

firefox-52.0-4.0.1.el7_3

163298 - Oracle Enterprise Linux ELSA-2017-0459 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
ELSA-2017-0459

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006775.html>

<http://oss.oracle.com/pipermail/el-errata/2017-March/006776.html>

OEL5

x86_64

firefox-45.8.0-2.0.1.el5_11

i386

firefox-45.8.0-2.0.1.el5_11

OEL6

x86_64

firefox-45.8.0-2.0.1.el6_8

i386

firefox-45.8.0-2.0.1.el6_8

175127 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x i386/x86_64 (1703-7158)

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x i386/x86_64 (1703-7158)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=7158>

SL6
x86_64
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

i386
firefox-45.8.0-2.el6_8
firefox-debuginfo-45.8.0-2.el6_8

SL5
x86_64
firefox-45.8.0-2.el5_11
firefox-debuginfo-45.8.0-2.el5_11

i386
firefox-45.8.0-2.el5_11
firefox-debuginfo-45.8.0-2.el5_11

175128 - Scientific Linux Security ERRATA Critical: firefox on SL7.x x86_64 (1703-6699)

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL7.x x86_64 (1703-6699)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=6699>

SL7
x86_64

firefox-debuginfo-52.0-4.el7_3
firefox-52.0-4.el7_3

21314 - (K03534020) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5767

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

Observation

F5's BIG-IP Products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the GD Graphics library used in PHP. Successful exploitation could allow an attacker to cause a denial of service condition or have other unspecified impact on the target system.

130720 - Debian Linux 8.0 DSA-3804-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9588, CVE-2017-2636, CVE-2017-5669, CVE-2017-5986, CVE-2017-6214, CVE-2017-6345, CVE-2017-6346, CVE-2017-6348, CVE-2017-6353

Description

The scan detected that the host is missing the following update:
DSA-3804-1

Observation

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

<http://www.debian.org/security/2017/dsa-3804>

Debian 8.0

all

udf-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
nic-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
scsi-core-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
linux-headers-3.16.0-4-octeon_3.16.39-1+deb8u2
xfs-modules-3.16.0-4-s390x-di_3.16.39-1+deb8u2
md-modules-3.16.0-4-powerpc64le-di_3.16.39-1+deb8u2
nic-wireless-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
xfs-modules-3.16.0-4-r4k-ip22-di_3.16.39-1+deb8u2
btrfs-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
affs-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
input-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
linux-image-3.16.0-4-arm64-dbg_3.16.39-1+deb8u2
cdrom-core-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
loop-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
event-modules-3.16.0-4-loongson-2f-di_3.16.39-1+deb8u2
input-modules-3.16.0-4-arm64-di_3.16.39-1+deb8u2
crypto-modules-3.16.0-4-armmp-di_3.16.39-1+deb8u2
nbd-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
nic-wireless-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2

linux-manual-3.16_3.16.39-1+deb8u2
isofs-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-versatile-di_3.16.39-1+deb8u2
usb-storage-modules-3.16.0-4-arm64-di_3.16.39-1+deb8u2
xfs-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
nbd-modules-3.16.0-4-r5k-ip32-di_3.16.39-1+deb8u2
pata-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
ppp-modules-3.16.0-4-versatile-di_3.16.39-1+deb8u2
squashfs-modules-3.16.0-4-armmp-di_3.16.39-1+deb8u2
multipath-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
md-modules-3.16.0-4-powerpc-di_3.16.39-1+deb8u2
linux-headers-3.16.0-4-orion5x_3.16.39-1+deb8u2
fuse-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
affs-modules-3.16.0-4-powerpc-di_3.16.39-1+deb8u2
xfs-modules-3.16.0-4-4kc-malta-di_3.16.39-1+deb8u2
kernel-image-3.16.0-4-r4k-ip22-di_3.16.39-1+deb8u2
pcmcia-storage-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
nic-shared-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
multipath-modules-3.16.0-4-kirkwood-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-686-pae-di_3.16.39-1+deb8u2
xfs-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-kirkwood-di_3.16.39-1+deb8u2
sata-modules-3.16.0-4-armmp-di_3.16.39-1+deb8u2
fuse-modules-3.16.0-4-powerpc64le-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-r5k-ip32-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-r4k-ip22-di_3.16.39-1+deb8u2
ata-modules-3.16.0-4-powerpc64le-di_3.16.39-1+deb8u2
leds-modules-3.16.0-4-kirkwood-di_3.16.39-1+deb8u2
crc-modules-3.16.0-4-r5k-ip32-di_3.16.39-1+deb8u2
input-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-armmp-di_3.16.39-1+deb8u2
jfs-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
scsi-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-powerpc64le-di_3.16.39-1+deb8u2
fb-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
fb-modules-3.16.0-4-kirkwood-di_3.16.39-1+deb8u2
crypto-modules-3.16.0-4-686-pae-di_3.16.39-1+deb8u2
linux-image-3.16.0-4-686-pae_3.16.39-1+deb8u2
virtio-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
serial-modules-3.16.0-4-586-di_3.16.39-1+deb8u2
pcmcia-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
linux-image-3.16.0-4-armmp_3.16.39-1+deb8u2
sata-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
kernel-image-3.16.0-4-s390x-di_3.16.39-1+deb8u2
loop-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
nic-modules-3.16.0-4-orion5x-di_3.16.39-1+deb8u2
sata-modules-3.16.0-4-686-pae-di_3.16.39-1+deb8u2
linux-image-3.16.0-4-amd64-dbg_3.16.39-1+deb8u2
fat-modules-3.16.0-4-586-di_3.16.39-1+deb8u2
mouse-modules-3.16.0-4-586-di_3.16.39-1+deb8u2
serial-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
cdrom-core-modules-3.16.0-4-586-di_3.16.39-1+deb8u2
hfs-modules-3.16.0-4-powerpc-di_3.16.39-1+deb8u2
mouse-modules-3.16.0-4-686-pae-di_3.16.39-1+deb8u2
nic-shared-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
cdrom-core-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
zlib-modules-3.16.0-4-r5k-ip32-di_3.16.39-1+deb8u2
pcmcia-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-586-di_3.16.39-1+deb8u2

ntfs-modules-3.16.0-4-loongson-2f-di_3.16.39-1+deb8u2
crc-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
scsi-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
nbd-modules-3.16.0-4-r4k-ip22-di_3.16.39-1+deb8u2
usb-storage-modules-3.16.0-4-loongson-2f-di_3.16.39-1+deb8u2
linux-image-3.16.0-4-r4k-ip22_3.16.39-1+deb8u2
minix-modules-3.16.0-4-loongson-2f-di_3.16.39-1+deb8u2
loop-modules-3.16.0-4-r4k-ip22-di_3.16.39-1+deb8u2
usb-storage-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
affs-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
nic-shared-modules-3.16.0-4-4kc-malta-di_3.16.39-1+deb8u2
linux-headers-3.16.0-4-all-armel_3.16.39-1+deb8u2
fat-modules-3.16.0-4-armmp-di_3.16.39-1+deb8u2
sata-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
crc-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
cdrom-core-modules-3.16.0-4-sb1-bcm91250a-di_3.16.39-1+deb8u2
md-modules-3.16.0-4-versatile-di_3.16.39-1+deb8u2
scsi-core-modules-3.16.0-4-586-di_3.16.39-1+deb8u2
event-modules-3.16.0-4-4kc-malta-di_3.16.39-1+deb8u2
kernel-image-3.16.0-4-octeon-di_3.16.39-1+deb8u2
efi-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
kernel-image-3.16.0-4-amd64-di_3.16.39-1+deb8u2
sound-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
minix-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-orion5x-di_3.16.39-1+deb8u2
md-modules-3.16.0-4-r4k-ip22-di_3.16.39-1+deb8u2
usb-modules-3.16.0-4-amd64-di_3.16.39-1+deb8u2
squashfs-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2
event-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
usb-storage-modules-3.16.0-4-powerpc-di_3.16.39-1+deb8u2
crypto-dm-modules-3.16.0-4-versatile-di_3.16.39-1+deb8u2
multipath-modules-3.16.0-4-loongson-2f-di_3.16.39-1+deb8u2
minix-modules-3.16.0-4-octeon-di_3.16.39-1+deb8u2
efi-modules-3.16.0-4-686-pae-di_3.16.39-1+deb8u2
affs-modules-3.16.0-4-4kc-malta-di_3.16.39-1+deb8u2
ppp-modules-3.16.0-4-orion5x-di_3.16.39-1+deb8u2
udf-modules-3.16.0-4-powerpc-di_3.16.39-1+deb8u2
pata-modules-3.16.0-4-4kc-malta-di_3.16.39-1+deb8u2
kernel-image-3.16.0-4-arm64-di_3.16.39-1+deb8u2
ext4-modules-3.16.0-4-versatile-di_3.16.39-1+deb8u2
usb-storage-modules-3.16.0-4-versatile-di_3.16.39-1+deb8u2
cdrom-core-modules-3.16.0-4-686-pae-di_3.16.39-1+deb8u2
md-modules-3.16.0-4-s390x-di_3.16.39-1+deb8u2
crypto-dm-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
nic-wireless-modules-3.16.0-4-loongson-3-di_3.16.39-1+deb8u2
pcmcia-storage-modules-3.16.0-4-powerpc-di_3.16.39-1+deb8u2
zlib-modules-3.16.0-4-4kc-malta-di_3.16.39-1+deb8u2
scsi-extra-modules-3.16.0-4-powerpc64-di_3.16.39-1+deb8u2
pcmcia-storage-modules-3.16.0-4-586-di_3.16.39-1+deb8u2
nbd-modules-3.16.0-4-arm64-di_3.16.39-1+deb8u2
hfs-modules-3.16.0-4-loongson-2e-di_3.16.39-1+deb8u2

141459 - Red Hat Enterprise Linux RHSA-2017-0501 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

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

RHSA-2017-0501

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0501.html>

RHEL7_2S

noarch

kernel-doc-3.10.0-327.49.2.el7

kernel-abi-whitelists-3.10.0-327.49.2.el7

x86_64

kernel-tools-libs-3.10.0-327.49.2.el7

perf-debuginfo-3.10.0-327.49.2.el7

kernel-debuginfo-common-x86_64-3.10.0-327.49.2.el7

perf-3.10.0-327.49.2.el7

kernel-debug-debuginfo-3.10.0-327.49.2.el7

kernel-debug-devel-3.10.0-327.49.2.el7

kernel-tools-3.10.0-327.49.2.el7

kernel-3.10.0-327.49.2.el7

kernel-tools-debuginfo-3.10.0-327.49.2.el7

python-perf-debuginfo-3.10.0-327.49.2.el7

kernel-debuginfo-3.10.0-327.49.2.el7

kernel-tools-libs-devel-3.10.0-327.49.2.el7

kernel-headers-3.10.0-327.49.2.el7

kernel-devel-3.10.0-327.49.2.el7

kernel-debug-3.10.0-327.49.2.el7

python-perf-3.10.0-327.49.2.el7

141461 - Red Hat Enterprise Linux RHSA-2017-0498 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

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

RHSA-2017-0498

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0498.html>

RHEL7S

x86_64

thunderbird-45.8.0-1.el7_3

thunderbird-debuginfo-45.8.0-1.el7_3

RHEL6S

i386

thunderbird-debuginfo-45.8.0-1.el6_8
thunderbird-45.8.0-1.el6_8

x86_64
thunderbird-debuginfo-45.8.0-1.el6_8
thunderbird-45.8.0-1.el6_8

RHEL6WS
x86_64
thunderbird-debuginfo-45.8.0-1.el6_8
thunderbird-45.8.0-1.el6_8

i386
thunderbird-debuginfo-45.8.0-1.el6_8
thunderbird-45.8.0-1.el6_8

RHEL5D
x86_64
thunderbird-45.8.0-1.el5_11
thunderbird-debuginfo-45.8.0-1.el5_11

i386
thunderbird-45.8.0-1.el5_11
thunderbird-debuginfo-45.8.0-1.el5_11

RHEL7D
x86_64
thunderbird-45.8.0-1.el7_3
thunderbird-debuginfo-45.8.0-1.el7_3

RHEL6D
x86_64
thunderbird-debuginfo-45.8.0-1.el6_8
thunderbird-45.8.0-1.el6_8

i386
thunderbird-debuginfo-45.8.0-1.el6_8
thunderbird-45.8.0-1.el6_8

RHEL7WS
x86_64
thunderbird-45.8.0-1.el7_3
thunderbird-debuginfo-45.8.0-1.el7_3

141463 - Red Hat Enterprise Linux RHSA-2017-0499 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5032, CVE-2017-5033, CVE-2017-5034, CVE-2017-5035, CVE-2017-5036, CVE-2017-5037, CVE-2017-5038, CVE-2017-5039, CVE-2017-5040, CVE-2017-5041, CVE-2017-5042, CVE-2017-5043, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

Description

The scan detected that the host is missing the following update:
RHSA-2017-0499

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0499.html>

RHEL6D

x86_64

chromium-browser-debuginfo-57.0.2987.98-1.el6

chromium-browser-57.0.2987.98-1.el6

i386

chromium-browser-debuginfo-57.0.2987.98-1.el6

chromium-browser-57.0.2987.98-1.el6

RHEL6S

x86_64

chromium-browser-debuginfo-57.0.2987.98-1.el6

chromium-browser-57.0.2987.98-1.el6

i386

chromium-browser-debuginfo-57.0.2987.98-1.el6

chromium-browser-57.0.2987.98-1.el6

RHEL6WS

x86_64

chromium-browser-debuginfo-57.0.2987.98-1.el6

chromium-browser-57.0.2987.98-1.el6

i386

chromium-browser-debuginfo-57.0.2987.98-1.el6

chromium-browser-57.0.2987.98-1.el6

141470 - Red Hat Enterprise Linux RHSA-2016-1096 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5364, CVE-2015-5366

Description

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

RHSA-2016-1096

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-1096.html>

RHEL6_4S

x86_64

kernel-debug-2.6.32-358.71.1.el6

python-perf-2.6.32-358.71.1.el6

kernel-debuginfo-2.6.32-358.71.1.el6

kernel-devel-2.6.32-358.71.1.el6

kernel-debuginfo-common-x86_64-2.6.32-358.71.1.el6

python-perf-debuginfo-2.6.32-358.71.1.el6

kernel-debug-devel-2.6.32-358.71.1.el6

perf-2.6.32-358.71.1.el6

kernel-debug-debuginfo-2.6.32-358.71.1.el6

kernel-headers-2.6.32-358.71.1.el6
perf-debuginfo-2.6.32-358.71.1.el6
kernel-2.6.32-358.71.1.el6

noarch
kernel-firmware-2.6.32-358.71.1.el6
kernel-doc-2.6.32-358.71.1.el6

141471 - Red Hat Enterprise Linux RHSA-2016-1814 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565, CVE-2016-5696

Description

The scan detected that the host is missing the following update:
RHSA-2016-1814

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1814.html>

RHEL6_5S
x86_64
kernel-debug-debuginfo-2.6.32-431.73.2.el6
kernel-debuginfo-2.6.32-431.73.2.el6
kernel-debuginfo-common-x86_64-2.6.32-431.73.2.el6
kernel-headers-2.6.32-431.73.2.el6
python-perf-2.6.32-431.73.2.el6
python-perf-debuginfo-2.6.32-431.73.2.el6
kernel-devel-2.6.32-431.73.2.el6
perf-debuginfo-2.6.32-431.73.2.el6
kernel-debug-devel-2.6.32-431.73.2.el6
kernel-debug-2.6.32-431.73.2.el6
kernel-2.6.32-431.73.2.el6
perf-2.6.32-431.73.2.el6

noarch
kernel-abi-whitelists-2.6.32-431.73.2.el6
kernel-doc-2.6.32-431.73.2.el6
kernel-firmware-2.6.32-431.73.2.el6

141472 - Red Hat Enterprise Linux RHSA-2016-1581 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565

Description

The scan detected that the host is missing the following update:
RHSA-2016-1581

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-1581.html>

RHEL6_4S

x86_64

kernel-headers-2.6.32-358.72.1.el6

python-perf-debuginfo-2.6.32-358.72.1.el6

kernel-debuginfo-common-x86_64-2.6.32-358.72.1.el6

kernel-debug-debuginfo-2.6.32-358.72.1.el6

perf-debuginfo-2.6.32-358.72.1.el6

kernel-debuginfo-2.6.32-358.72.1.el6

kernel-debug-2.6.32-358.72.1.el6

kernel-2.6.32-358.72.1.el6

python-perf-2.6.32-358.72.1.el6

kernel-devel-2.6.32-358.72.1.el6

perf-2.6.32-358.72.1.el6

kernel-debug-devel-2.6.32-358.72.1.el6

noarch

kernel-firmware-2.6.32-358.72.1.el6

kernel-doc-2.6.32-358.72.1.el6

141473 - Red Hat Enterprise Linux RHSA-2016-0103 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1805, CVE-2015-8104, CVE-2016-0728, CVE-2016-0774

Description

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

RHSA-2016-0103

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0103.html>

RHEL7_1S

noarch

kernel-abi-whitelists-3.10.0-229.26.2.el7

kernel-doc-3.10.0-229.26.2.el7

x86_64

perf-debuginfo-3.10.0-229.26.2.el7

kernel-3.10.0-229.26.2.el7

kernel-headers-3.10.0-229.26.2.el7

kernel-tools-3.10.0-229.26.2.el7

kernel-debuginfo-common-x86_64-3.10.0-229.26.2.el7

kernel-debug-debuginfo-3.10.0-229.26.2.el7

kernel-tools-debuginfo-3.10.0-229.26.2.el7

kernel-debug-devel-3.10.0-229.26.2.el7

kernel-tools-libs-devel-3.10.0-229.26.2.el7

kernel-debug-3.10.0-229.26.2.el7

kernel-tools-libs-3.10.0-229.26.2.el7

python-perf-3.10.0-229.26.2.el7

kernel-debuginfo-3.10.0-229.26.2.el7

python-perf-debuginfo-3.10.0-229.26.2.el7
perf-3.10.0-229.26.2.el7
kernel-devel-3.10.0-229.26.2.el7

141474 - Red Hat Enterprise Linux RHSA-2016-2133 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4470, CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2133

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2133.html>

RHEL6_4S
x86_64
kernel-debug-2.6.32-358.75.1.el6
perf-debuginfo-2.6.32-358.75.1.el6
kernel-headers-2.6.32-358.75.1.el6
kernel-devel-2.6.32-358.75.1.el6
kernel-debug-debuginfo-2.6.32-358.75.1.el6
python-perf-2.6.32-358.75.1.el6
kernel-debug-devel-2.6.32-358.75.1.el6
kernel-2.6.32-358.75.1.el6
perf-2.6.32-358.75.1.el6
kernel-debuginfo-2.6.32-358.75.1.el6
python-perf-debuginfo-2.6.32-358.75.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.75.1.el6

noarch
kernel-firmware-2.6.32-358.75.1.el6
kernel-doc-2.6.32-358.75.1.el6

141475 - Red Hat Enterprise Linux RHSA-2016-2126 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2126

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2126.html>

RHEL5_9S

i386
kernel-2.6.18-348.32.1.el5
kernel-PAE-2.6.18-348.32.1.el5
kernel-debuginfo-common-2.6.18-348.32.1.el5
kernel-debuginfo-2.6.18-348.32.1.el5
kernel-debug-debuginfo-2.6.18-348.32.1.el5
kernel-devel-2.6.18-348.32.1.el5
kernel-xen-2.6.18-348.32.1.el5
kernel-debug-2.6.18-348.32.1.el5
kernel-PAE-devel-2.6.18-348.32.1.el5
kernel-xen-devel-2.6.18-348.32.1.el5
kernel-PAE-debuginfo-2.6.18-348.32.1.el5
kernel-headers-2.6.18-348.32.1.el5
kernel-debug-devel-2.6.18-348.32.1.el5
kernel-xen-debuginfo-2.6.18-348.32.1.el5

noarch
kernel-doc-2.6.18-348.32.1.el5

x86_64
kernel-xen-devel-2.6.18-348.32.1.el5
kernel-xen-2.6.18-348.32.1.el5
kernel-debug-debuginfo-2.6.18-348.32.1.el5
kernel-headers-2.6.18-348.32.1.el5
kernel-devel-2.6.18-348.32.1.el5
kernel-2.6.18-348.32.1.el5
kernel-debuginfo-common-2.6.18-348.32.1.el5
kernel-debug-2.6.18-348.32.1.el5
kernel-xen-debuginfo-2.6.18-348.32.1.el5
kernel-debug-devel-2.6.18-348.32.1.el5
kernel-debuginfo-2.6.18-348.32.1.el5

141476 - Red Hat Enterprise Linux RHSA-2016-2106 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2106

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2106.html>

RHEL6_7S
i386
python-perf-2.6.32-573.35.2.el6
kernel-devel-2.6.32-573.35.2.el6
perf-2.6.32-573.35.2.el6
perf-debuginfo-2.6.32-573.35.2.el6
kernel-2.6.32-573.35.2.el6
kernel-debug-2.6.32-573.35.2.el6
kernel-debuginfo-common-i686-2.6.32-573.35.2.el6
kernel-debuginfo-2.6.32-573.35.2.el6

kernel-debug-devel-2.6.32-573.35.2.el6
kernel-debug-debuginfo-2.6.32-573.35.2.el6
kernel-headers-2.6.32-573.35.2.el6
python-perf-debuginfo-2.6.32-573.35.2.el6

noarch
kernel-firmware-2.6.32-573.35.2.el6
kernel-doc-2.6.32-573.35.2.el6
kernel-abi-whitelists-2.6.32-573.35.2.el6

x86_64
python-perf-2.6.32-573.35.2.el6
kernel-devel-2.6.32-573.35.2.el6
kernel-headers-2.6.32-573.35.2.el6
python-perf-debuginfo-2.6.32-573.35.2.el6
kernel-debuginfo-2.6.32-573.35.2.el6
perf-debuginfo-2.6.32-573.35.2.el6
kernel-debug-debuginfo-2.6.32-573.35.2.el6
kernel-debug-devel-2.6.32-573.35.2.el6
kernel-debuginfo-common-i686-2.6.32-573.35.2.el6
kernel-debug-2.6.32-573.35.2.el6
kernel-2.6.32-573.35.2.el6
kernel-debuginfo-common-x86_64-2.6.32-573.35.2.el6
perf-2.6.32-573.35.2.el6

141477 - Red Hat Enterprise Linux RHSA-2016-1225 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5364, CVE-2015-5366

Description

The scan detected that the host is missing the following update:
RHSA-2016-1225

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00007.html>

RHEL6_5S
x86_64
kernel-debuginfo-2.6.32-431.72.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.72.1.el6
kernel-devel-2.6.32-431.72.1.el6
python-perf-2.6.32-431.72.1.el6
perf-debuginfo-2.6.32-431.72.1.el6
kernel-debug-debuginfo-2.6.32-431.72.1.el6
kernel-2.6.32-431.72.1.el6
kernel-debug-2.6.32-431.72.1.el6
python-perf-debuginfo-2.6.32-431.72.1.el6
kernel-debug-devel-2.6.32-431.72.1.el6
perf-2.6.32-431.72.1.el6
kernel-headers-2.6.32-431.72.1.el6

noarch
kernel-firmware-2.6.32-431.72.1.el6

kernel-doc-2.6.32-431.72.1.el6
kernel-abi-whitelists-2.6.32-431.72.1.el6

141478 - Red Hat Enterprise Linux RHSA-2016-1657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4470, CVE-2016-4565, CVE-2016-5696

Description

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

RHSA-2016-1657

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-1657.html>

RHEL7_1S

noarch

kernel-doc-3.10.0-229.40.1.el7

kernel-abi-whitelists-3.10.0-229.40.1.el7

x86_64

kernel-debuginfo-common-x86_64-3.10.0-229.40.1.el7

kernel-headers-3.10.0-229.40.1.el7

kernel-tools-debuginfo-3.10.0-229.40.1.el7

python-perf-3.10.0-229.40.1.el7

kernel-debug-debuginfo-3.10.0-229.40.1.el7

python-perf-debuginfo-3.10.0-229.40.1.el7

kernel-debug-devel-3.10.0-229.40.1.el7

kernel-3.10.0-229.40.1.el7

kernel-tools-libs-devel-3.10.0-229.40.1.el7

kernel-debug-3.10.0-229.40.1.el7

perf-debuginfo-3.10.0-229.40.1.el7

kernel-tools-3.10.0-229.40.1.el7

kernel-devel-3.10.0-229.40.1.el7

perf-3.10.0-229.40.1.el7

kernel-debuginfo-3.10.0-229.40.1.el7

kernel-tools-libs-3.10.0-229.40.1.el7

141483 - Red Hat Enterprise Linux RHSA-2016-2127 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

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

RHSA-2016-2127

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2127.html>

RHEL5_6S

i386

kernel-xen-2.6.18-238.57.1.el5
kernel-debug-2.6.18-238.57.1.el5
kernel-xen-debuginfo-2.6.18-238.57.1.el5
kernel-debug-debuginfo-2.6.18-238.57.1.el5
kernel-debuginfo-2.6.18-238.57.1.el5
kernel-headers-2.6.18-238.57.1.el5
kernel-debuginfo-common-2.6.18-238.57.1.el5
kernel-PAE-2.6.18-238.57.1.el5
kernel-2.6.18-238.57.1.el5
kernel-PAE-devel-2.6.18-238.57.1.el5
kernel-debug-devel-2.6.18-238.57.1.el5
kernel-PAE-debuginfo-2.6.18-238.57.1.el5
kernel-xen-devel-2.6.18-238.57.1.el5
kernel-devel-2.6.18-238.57.1.el5

noarch

kernel-doc-2.6.18-238.57.1.el5

x86_64

kernel-xen-debuginfo-2.6.18-238.57.1.el5
kernel-2.6.18-238.57.1.el5
kernel-debuginfo-2.6.18-238.57.1.el5
kernel-devel-2.6.18-238.57.1.el5
kernel-headers-2.6.18-238.57.1.el5
kernel-debug-devel-2.6.18-238.57.1.el5
kernel-xen-2.6.18-238.57.1.el5
kernel-debug-debuginfo-2.6.18-238.57.1.el5
kernel-debuginfo-common-2.6.18-238.57.1.el5
kernel-debug-2.6.18-238.57.1.el5
kernel-xen-devel-2.6.18-238.57.1.el5

141484 - Red Hat Enterprise Linux RHSA-2016-1489 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565

Description

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

RHSA-2016-1489

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-1489.html>

RHEL6_7S

i386

kernel-debug-debuginfo-2.6.32-573.32.1.el6
kernel-headers-2.6.32-573.32.1.el6
perf-debuginfo-2.6.32-573.32.1.el6
kernel-debug-devel-2.6.32-573.32.1.el6
kernel-debuginfo-2.6.32-573.32.1.el6

python-perf-debuginfo-2.6.32-573.32.1.el6
kernel-2.6.32-573.32.1.el6
perf-2.6.32-573.32.1.el6
kernel-debug-2.6.32-573.32.1.el6
kernel-devel-2.6.32-573.32.1.el6
python-perf-2.6.32-573.32.1.el6
kernel-debuginfo-common-i686-2.6.32-573.32.1.el6

noarch
kernel-firmware-2.6.32-573.32.1.el6
kernel-abi-whitelists-2.6.32-573.32.1.el6
kernel-doc-2.6.32-573.32.1.el6

x86_64
kernel-debug-2.6.32-573.32.1.el6
kernel-headers-2.6.32-573.32.1.el6
kernel-debuginfo-2.6.32-573.32.1.el6
python-perf-debuginfo-2.6.32-573.32.1.el6
kernel-debuginfo-common-i686-2.6.32-573.32.1.el6
perf-2.6.32-573.32.1.el6
kernel-debug-devel-2.6.32-573.32.1.el6
kernel-devel-2.6.32-573.32.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.32.1.el6
perf-debuginfo-2.6.32-573.32.1.el6
kernel-debug-debuginfo-2.6.32-573.32.1.el6
kernel-2.6.32-573.32.1.el6
python-perf-2.6.32-573.32.1.el6

141486 - Red Hat Enterprise Linux RHSA-2016-0078 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000

Description

The scan detected that the host is missing the following update:
RHSA-2016-0078

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0078.html>

RHEL6_5S

i386
bind-9.8.2-0.23.rc1.el6_5.2
bind-chroot-9.8.2-0.23.rc1.el6_5.2
bind-utils-9.8.2-0.23.rc1.el6_5.2
bind-sdb-9.8.2-0.23.rc1.el6_5.2
bind-libs-9.8.2-0.23.rc1.el6_5.2
bind-debuginfo-9.8.2-0.23.rc1.el6_5.2
bind-devel-9.8.2-0.23.rc1.el6_5.2

x86_64

bind-9.8.2-0.23.rc1.el6_5.2
bind-chroot-9.8.2-0.23.rc1.el6_5.2
bind-utils-9.8.2-0.23.rc1.el6_5.2

bind-sdb-9.8.2-0.23.rc1.el6_5.2
bind-libs-9.8.2-0.23.rc1.el6_5.2
bind-debuginfo-9.8.2-0.23.rc1.el6_5.2
bind-devel-9.8.2-0.23.rc1.el6_5.2

RHEL6_4S

i386
bind-9.8.2-0.17.rc1.el6_4.7
bind-sdb-9.8.2-0.17.rc1.el6_4.7
bind-chroot-9.8.2-0.17.rc1.el6_4.7
bind-devel-9.8.2-0.17.rc1.el6_4.7
bind-utils-9.8.2-0.17.rc1.el6_4.7
bind-libs-9.8.2-0.17.rc1.el6_4.7
bind-debuginfo-9.8.2-0.17.rc1.el6_4.7

x86_64

bind-9.8.2-0.17.rc1.el6_4.7
bind-sdb-9.8.2-0.17.rc1.el6_4.7
bind-chroot-9.8.2-0.17.rc1.el6_4.7
bind-devel-9.8.2-0.17.rc1.el6_4.7
bind-utils-9.8.2-0.17.rc1.el6_4.7
bind-libs-9.8.2-0.17.rc1.el6_4.7
bind-debuginfo-9.8.2-0.17.rc1.el6_4.7

141488 - Red Hat Enterprise Linux RHSA-2016-2120 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2120

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2120.html>

RHEL6_5S

x86_64
kernel-debuginfo-2.6.32-431.75.1.el6
perf-2.6.32-431.75.1.el6
python-perf-2.6.32-431.75.1.el6
kernel-debug-2.6.32-431.75.1.el6
kernel-headers-2.6.32-431.75.1.el6
kernel-2.6.32-431.75.1.el6
kernel-devel-2.6.32-431.75.1.el6
kernel-debug-debuginfo-2.6.32-431.75.1.el6
kernel-debug-devel-2.6.32-431.75.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.75.1.el6
perf-debuginfo-2.6.32-431.75.1.el6
python-perf-debuginfo-2.6.32-431.75.1.el6

noarch

kernel-doc-2.6.32-431.75.1.el6
kernel-firmware-2.6.32-431.75.1.el6

141492 - Red Hat Enterprise Linux RHSA-2016-2695 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3841

Description

The scan detected that the host is missing the following update:
RHSA-2016-2695

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2695.html>

RHEL7_2S

noarch

kernel-abi-whitelists-3.10.0-327.41.3.el7

kernel-doc-3.10.0-327.41.3.el7

x86_64

kernel-debug-debuginfo-3.10.0-327.41.3.el7

kernel-debug-3.10.0-327.41.3.el7

kernel-tools-3.10.0-327.41.3.el7

python-perf-3.10.0-327.41.3.el7

kernel-3.10.0-327.41.3.el7

kernel-tools-libs-3.10.0-327.41.3.el7

kernel-tools-debuginfo-3.10.0-327.41.3.el7

kernel-debuginfo-common-x86_64-3.10.0-327.41.3.el7

kernel-headers-3.10.0-327.41.3.el7

perf-3.10.0-327.41.3.el7

kernel-debuginfo-3.10.0-327.41.3.el7

python-perf-debuginfo-3.10.0-327.41.3.el7

kernel-devel-3.10.0-327.41.3.el7

kernel-tools-libs-devel-3.10.0-327.41.3.el7

kernel-debug-devel-3.10.0-327.41.3.el7

perf-debuginfo-3.10.0-327.41.3.el7

141495 - Red Hat Enterprise Linux RHSA-2016-2118 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2118

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2118.html>

RHEL7_1S
noarch
kernel-abi-whitelists-3.10.0-229.42.2.el7
kernel-doc-3.10.0-229.42.2.el7

x86_64
kernel-tools-libs-devel-3.10.0-229.42.2.el7
kernel-debuginfo-common-x86_64-3.10.0-229.42.2.el7
kernel-tools-debuginfo-3.10.0-229.42.2.el7
kernel-devel-3.10.0-229.42.2.el7
perf-debuginfo-3.10.0-229.42.2.el7
perf-3.10.0-229.42.2.el7
kernel-tools-libs-3.10.0-229.42.2.el7
kernel-debuginfo-3.10.0-229.42.2.el7
kernel-tools-3.10.0-229.42.2.el7
kernel-debug-debuginfo-3.10.0-229.42.2.el7
kernel-debug-devel-3.10.0-229.42.2.el7
python-perf-3.10.0-229.42.2.el7
kernel-3.10.0-229.42.2.el7
kernel-headers-3.10.0-229.42.2.el7
kernel-debug-3.10.0-229.42.2.el7
python-perf-debuginfo-3.10.0-229.42.2.el7

141498 - Red Hat Enterprise Linux RHSA-2015-2589 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, CVE-2015-5277

Description

The scan detected that the host is missing the following update:
RHSA-2015-2589

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2589.html>

RHEL7_1S
x86_64
glibc-headers-2.17-79.el7_1
glibc-static-2.17-79.el7_1
glibc-debuginfo-2.17-79.el7_1
glibc-2.17-79.el7_1
glibc-common-2.17-79.el7_1
glibc-devel-2.17-79.el7_1
glibc-debuginfo-common-2.17-79.el7_1
nscd-2.17-79.el7_1
glibc-utils-2.17-79.el7_1

141500 - Red Hat Enterprise Linux RHSA-2015-0629 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0822, CVE-2015-0827, CVE-2015-0831, CVE-2015-0836

Description

The scan detected that the host is missing the following update:
RHSA-2015-0629

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-0629.html>

RHEL7S
ppc64le
firefox-31.5.0-2.ael7b_1
firefox-debuginfo-31.5.0-2.ael7b_1

141502 - Red Hat Enterprise Linux RHSA-2015-1211 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1805

Description

The scan detected that the host is missing the following update:
RHSA-2015-1211

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-1211.html>

RHEL6_4S
i386
kernel-debug-devel-2.6.32-358.62.1.el6
kernel-debuginfo-2.6.32-358.62.1.el6
kernel-debuginfo-common-i686-2.6.32-358.62.1.el6
kernel-2.6.32-358.62.1.el6
kernel-debug-debuginfo-2.6.32-358.62.1.el6
perf-debuginfo-2.6.32-358.62.1.el6
python-perf-debuginfo-2.6.32-358.62.1.el6
python-perf-2.6.32-358.62.1.el6
perf-2.6.32-358.62.1.el6
kernel-headers-2.6.32-358.62.1.el6
kernel-devel-2.6.32-358.62.1.el6
kernel-debug-2.6.32-358.62.1.el6

noarch
kernel-doc-2.6.32-358.62.1.el6
kernel-firmware-2.6.32-358.62.1.el6

x86_64
kernel-debug-devel-2.6.32-358.62.1.el6
kernel-debuginfo-2.6.32-358.62.1.el6
kernel-headers-2.6.32-358.62.1.el6
kernel-2.6.32-358.62.1.el6
kernel-debug-debuginfo-2.6.32-358.62.1.el6

perf-debuginfo-2.6.32-358.62.1.el6
python-perf-debuginfo-2.6.32-358.62.1.el6
python-perf-2.6.32-358.62.1.el6
perf-2.6.32-358.62.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.62.1.el6
kernel-devel-2.6.32-358.62.1.el6
kernel-debug-2.6.32-358.62.1.el6

145250 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0607-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10009, CVE-2016-10011, CVE-2016-8858

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0607-2

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002685.html>

SuSE SLES 12 SP1

ppc64le
openssh-askpass-gnome-debuginfo-6.6p1-54.7.1
openssh-6.6p1-54.7.1
openssh-helpers-debuginfo-6.6p1-54.7.1
openssh-debuginfo-6.6p1-54.7.1
openssh-debugsource-6.6p1-54.7.1
openssh-fips-6.6p1-54.7.1
openssh-helpers-6.6p1-54.7.1
openssh-askpass-gnome-6.6p1-54.7.1

SuSE SLED 12 SP1

x86_64
openssh-askpass-gnome-debuginfo-6.6p1-54.7.1
openssh-6.6p1-54.7.1
openssh-helpers-debuginfo-6.6p1-54.7.1
openssh-debuginfo-6.6p1-54.7.1
openssh-debugsource-6.6p1-54.7.1
openssh-helpers-6.6p1-54.7.1
openssh-askpass-gnome-6.6p1-54.7.1

145252 - SuSE SLES 11 SP4 SUSE-SU-2017:0656-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7922, CVE-2016-7923, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7931, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486

Description

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

SUSE-SU-2017:0656-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002691.html>

SuSE SLES 11 SP4
i586
tcpdump-3.9.8-1.29.1

x86_64
tcpdump-3.9.8-1.29.1

145253 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0641-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8637

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0641-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002688.html>

SuSE SLES 12 SP1
x86_64
dracut-debugsource-037-91.1
dracut-debuginfo-037-91.1
dracut-037-91.1
dracut-fips-037-91.1

SuSE SLED 12 SP1
x86_64
dracut-debugsource-037-91.1
dracut-debuginfo-037-91.1
dracut-037-91.1

160224 - CentOS 5 CESA-2017-0454 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
CESA-2017-0454

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022325.html>

CentOS 5
x86_64
kmod-kvm-83-277.el5.centos
kvm-83-277.el5.centos
kmod-kvm-debug-83-277.el5.centos
kvm-tools-83-277.el5.centos
kvm-qemu-img-83-277.el5.centos

163297 - Oracle Enterprise Linux ELSA-2017-0498 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636, CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
ELSA-2017-0498

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006783.html>
<http://oss.oracle.com/pipermail/el-errata/2017-March/006784.html>

OEL7
x86_64
thunderbird-45.8.0-1.0.1.el7_3

OEL6
x86_64
thunderbird-45.8.0-1.0.1.el6_8

i386
thunderbird-45.8.0-1.0.1.el6_8

175126 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1703-7630)

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1703-7630)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=7630>

SL5

x86_64

thunderbird-45.8.0-1.el5_11

thunderbird-debuginfo-45.8.0-1.el5_11

i386

thunderbird-45.8.0-1.el5_11

thunderbird-debuginfo-45.8.0-1.el5_11

SL7

x86_64

thunderbird-45.8.0-1.el7_3

thunderbird-debuginfo-45.8.0-1.el7_3

SL6

x86_64

thunderbird-debuginfo-45.8.0-1.el6_8

thunderbird-45.8.0-1.el6_8

i386

thunderbird-debuginfo-45.8.0-1.el6_8

thunderbird-45.8.0-1.el6_8

185610 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3225-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5418, CVE-2016-6250, CVE-2016-7166, CVE-2016-8687, CVE-2016-8688, CVE-2016-8689, CVE-2017-5601

Description

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

USN-3225-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003769.html>

Ubuntu 12.04

libarchive12_3.0.3-6ubuntu1.4

Ubuntu 16.04

libarchive13_3.1.2-11ubuntu0.16.04.3

Ubuntu 14.04

libarchive13_3.1.2-7ubuntu2.4

Ubuntu 16.10

libarchive13_3.2.1-2ubuntu0.1

185611 - Ubuntu Linux 16.10 USN-3221-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3221-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003763.html>

Ubuntu 16.10

linux-image-4.8.0-41-generic_4.8.0-41.44
linux-image-generic_4.8.0.41.52
linux-image-4.8.0-41-powerpc-smp_4.8.0-41.44
linux-image-4.8.0-41-generic-lpae_4.8.0-41.44
linux-image-4.8.0-1028-raspi2_4.8.0-1028.31
linux-image-powerpc-e500mc_4.8.0.41.52
linux-image-raspi2_4.8.0.1028.31
linux-image-powerpc64-emb_4.8.0.41.52
linux-image-generic-lpae_4.8.0.41.52
linux-image-4.8.0-41-lowlatency_4.8.0-41.44
linux-image-4.8.0-41-powerpc64-emb_4.8.0-41.44
linux-image-lowlatency_4.8.0.41.52
linux-image-powerpc-smp_4.8.0.41.52
linux-image-4.8.0-41-powerpc-e500mc_4.8.0-41.44

185612 - Ubuntu Linux 12.04 USN-3218-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3218-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003758.html>

Ubuntu 12.04

linux-image-generic-pae_3.2.0.124.139
linux-image-3.2.0-124-powerpc-smp_3.2.0-124.167
linux-image-3.2.0-1502-omap4_3.2.0-1502.129
linux-image-highbank_3.2.0.124.139
linux-image-3.2.0-124-virtual_3.2.0-124.167

linux-image-3.2.0-124-powerpc64-smp_3.2.0-124.167
linux-image-powerpc64-smp_3.2.0.124.139
linux-image-omap4_3.2.0.1502.97
linux-image-3.2.0-124-generic-pae_3.2.0-124.167
linux-image-virtual_3.2.0.124.139
linux-image-powerpc-smp_3.2.0.124.139
linux-image-generic_3.2.0.124.139
linux-image-3.2.0-124-generic_3.2.0-124.167
linux-image-3.2.0-124-highbank_3.2.0-124.167
linux-image-omap_3.2.0.124.139
linux-image-3.2.0-124-omap_3.2.0-124.167

185614 - Ubuntu Linux 14.04 USN-3219-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3219-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003759.html>

Ubuntu 14.04

linux-image-powerpc-e500_3.13.0.112.120
linux-image-powerpc-smp_3.13.0.112.120
linux-image-generic-lpae_3.13.0.112.120
linux-image-3.13.0-112-powerpc-smp_3.13.0-112.159
linux-image-powerpc64-smp_3.13.0.112.120
linux-image-3.13.0-112-powerpc64-emb_3.13.0-112.159
linux-image-3.13.0-112-lowlatency_3.13.0-112.159
linux-image-generic_3.13.0.112.120
linux-image-3.13.0-112-generic_3.13.0-112.159
linux-image-3.13.0-112-powerpc-e500_3.13.0-112.159
linux-image-3.13.0-112-generic-lpae_3.13.0-112.159
linux-image-3.13.0-112-powerpc-e500mc_3.13.0-112.159
linux-image-lowlatency_3.13.0.112.120
linux-image-powerpc64-emb_3.13.0.112.120
linux-image-powerpc-e500mc_3.13.0.112.120
linux-image-3.13.0-112-powerpc64-smp_3.13.0-112.159

185615 - Ubuntu Linux 16.04 USN-3221-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3221-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003764.html>

Ubuntu 16.04

linux-image-4.8.0-41-powerpc-e500mc_4.8.0-41.44~16.04.1
linux-image-lowlatency-hwe-16.04_4.8.0.41.12
linux-image-4.8.0-41-generic-lpae_4.8.0-41.44~16.04.1
linux-image-generic-hwe-16.04_4.8.0.41.12
linux-image-4.8.0-41-generic_4.8.0-41.44~16.04.1
linux-image-4.8.0-41-powerpc-smp_4.8.0-41.44~16.04.1
linux-image-4.8.0-41-lowlatency_4.8.0-41.44~16.04.1
linux-image-4.8.0-41-powerpc64-emb_4.8.0-41.44~16.04.1
linux-image-generic-lpae-hwe-16.04_4.8.0.41.12

185616 - Ubuntu Linux 14.04 USN-3220-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3220-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003762.html>

Ubuntu 14.04

linux-image-4.4.0-66-powerpc64-smp_4.4.0-66.87~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.66.52
linux-image-generic-lts-xenial_4.4.0.66.52
linux-image-4.4.0-66-generic-lpae_4.4.0-66.87~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.66.52
linux-image-4.4.0-66-generic_4.4.0-66.87~14.04.1
linux-image-4.4.0-66-lowlatency_4.4.0-66.87~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.66.52
linux-image-4.4.0-66-powerpc-smp_4.4.0-66.87~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.66.52
linux-image-4.4.0-66-powerpc64-emb_4.4.0-66.87~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.66.52
linux-image-powerpc64-emb-lts-xenial_4.4.0.66.52
linux-image-4.4.0-66-powerpc-e500mc_4.4.0-66.87~14.04.1

185620 - Ubuntu Linux 16.04 USN-3220-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3220-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003761.html>

Ubuntu 16.04

linux-image-4.4.0-66-powerpc-e500mc_4.4.0-66.87
linux-image-powerpc64-smp_4.4.0.66.70
linux-image-lowlatency_4.4.0.66.70
linux-image-4.4.0-66-powerpc-smp_4.4.0-66.87
linux-image-gke_4.4.0.1005.5
linux-image-powerpc64-emb_4.4.0.66.70
linux-image-4.4.0-1046-raspi2_4.4.0-1046.53
linux-image-snapdragon_4.4.0.1050.42
linux-image-powerpc-smp_4.4.0.66.70
linux-image-raspi2_4.4.0.1046.45
linux-image-4.4.0-1050-snapdragon_4.4.0-1050.54
linux-image-4.4.0-1005-gke_4.4.0-1005.6
linux-image-generic_4.4.0.66.70
linux-image-4.4.0-66-lowlatency_4.4.0-66.87
linux-image-generic-lpae_4.4.0.66.70
linux-image-powerpc-e500mc_4.4.0.66.70
linux-image-4.4.0-66-generic-lpae_4.4.0-66.87
linux-image-4.4.0-66-powerpc64-emb_4.4.0-66.87
linux-image-4.4.0-66-generic_4.4.0-66.87
linux-image-4.4.0-66-powerpc64-smp_4.4.0-66.87

185621 - Ubuntu Linux 16.04 USN-3220-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
USN-3220-3

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003766.html>

Ubuntu 16.04

linux-image-aws_4.4.0.1007.8
linux-image-4.4.0-1007-aws_4.4.0-1007.16

185623 - Ubuntu Linux 12.04 USN-3219-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

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

USN-3219-2

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003760.html>

Ubuntu 12.04

linux-image-3.13.0-112-generic_3.13.0-112.159~precise1

linux-image-generic-lts-trusty_3.13.0.112.103

linux-image-3.13.0-112-generic-lpae_3.13.0-112.159~precise1

linux-image-generic-lpae-lts-trusty_3.13.0.112.103

191801 - Fedora Linux 25 FEDORA-2017-2c29702300 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6255, CVE-2016-8863

Description

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

FEDORA-2017-2c29702300

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

libupnp-1.6.21-1.fc25

191806 - Fedora Linux 25 FEDORA-2017-c3739273e5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5884, CVE-2017-5885

Description

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

FEDORA-2017-c3739273e5

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

mingw-gtk-vnc-0.7.0-1.fc25

191808 - Fedora Linux 24 FEDORA-2017-2e1f3694b2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5669, CVE-2017-5986, CVE-2017-6353

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2e1f3694b2

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

kernel-4.9.13-101.fc24

191809 - Fedora Linux 24 FEDORA-2017-d2bab54ac9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d2bab54ac9

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

GraphicsMagick-1.3.25-6.fc24

191811 - Fedora Linux 25 FEDORA-2017-387ff46a66 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5669, CVE-2017-5986, CVE-2017-6353

Description

The scan detected that the host is missing the following update:
FEDORA-2017-387ff46a66

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

kernel-4.9.13-201.fc25

191815 - Fedora Linux 24 FEDORA-2017-404f1a29fc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5884, CVE-2017-5885

Description

The scan detected that the host is missing the following update:
FEDORA-2017-404f1a29fc

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

mingw-gtk-vnc-0.7.0-1.fc24

191816 - Fedora Linux 25 FEDORA-2017-6c91c98b33 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6467, CVE-2017-6468, CVE-2017-6469, CVE-2017-6470, CVE-2017-6471, CVE-2017-6472, CVE-2017-6473, CVE-2017-6474

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6c91c98b33

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

wireshark-2.2.5-1.fc25

191818 - Fedora Linux 25 FEDORA-2017-c71a0f40f0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c71a0f40f0

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

GraphicsMagick-1.3.25-6.fc25

191827 - Fedora Linux 24 FEDORA-2017-3bd0b2e2c0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6255, CVE-2016-8863

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3bd0b2e2c0

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

libupnp-1.6.21-1.fc24

191835 - Fedora Linux 24 FEDORA-2017-9a5b89363f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10166, CVE-2016-10167, CVE-2016-10168, CVE-2016-6912, CVE-2016-9317

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9a5b89363f

Observation

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

Fedora Core 24

libwmf-0.2.8.4-50.fc24

141466 - Red Hat Enterprise Linux RHSA-2016-0618 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

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

RHSA-2016-0618

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0618.html>

RHEL7_1S

noarch

samba-pidl-4.2.10-5.el7_1

openchange-devel-docs-2.0-4.el7_1.1

samba-common-4.2.10-5.el7_1

x86_64

samba-vfs-glusterfs-4.2.10-5.el7_1

libwbclient-devel-4.2.10-5.el7_1

samba-client-4.2.10-5.el7_1

libtalloc-2.1.5-1.el7_1

pytalloc-devel-2.1.5-1.el7_1

samba-dc-libs-4.2.10-5.el7_1

libwbclient-4.2.10-5.el7_1

libsmbclient-devel-4.2.10-5.el7_1

ipa-client-4.1.0-18.el7_1.6

python-tevent-0.9.26-1.el7_1

libtevent-0.9.26-1.el7_1

samba-debuginfo-4.2.10-5.el7_1

openchange-2.0-4.el7_1.1

libldb-devel-1.1.25-1.el7_1

ipa-server-trust-ad-4.1.0-18.el7_1.6

samba-winbind-clients-4.2.10-5.el7_1

pytalloc-2.1.5-1.el7_1

pyldb-1.1.25-1.el7_1

libtdb-debuginfo-1.3.8-1.el7_1

libtalloc-devel-2.1.5-1.el7_1

openchange-debuginfo-2.0-4.el7_1.1

samba-winbind-4.2.10-5.el7_1

libtdb-devel-1.3.8-1.el7_1

samba-test-devel-4.2.10-5.el7_1

samba-dc-4.2.10-5.el7_1

tdb-tools-1.3.8-1.el7_1

libldb-1.1.25-1.el7_1

samba-common-libs-4.2.10-5.el7_1

libsmbclient-4.2.10-5.el7_1
samba-test-4.2.10-5.el7_1
pyldb-devel-1.1.25-1.el7_1
samba-python-4.2.10-5.el7_1
samba-winbind-krb5-locator-4.2.10-5.el7_1
samba-devel-4.2.10-5.el7_1
python-tdb-1.3.8-1.el7_1
ipa-python-4.1.0-18.el7_1.6
samba-4.2.10-5.el7_1
libtalloc-debuginfo-2.1.5-1.el7_1
openchange-client-2.0-4.el7_1.1
samba-common-tools-4.2.10-5.el7_1
samba-winbind-modules-4.2.10-5.el7_1
libtevent-devel-0.9.26-1.el7_1
samba-client-libs-4.2.10-5.el7_1
openchange-devel-2.0-4.el7_1.1
ipa-debuginfo-4.1.0-18.el7_1.6
ldb-tools-1.1.25-1.el7_1
samba-test-libs-4.2.10-5.el7_1
samba-libs-4.2.10-5.el7_1
ipa-admintools-4.1.0-18.el7_1.6
libldb-debuginfo-1.1.25-1.el7_1
libtevent-debuginfo-0.9.26-1.el7_1
ipa-server-4.1.0-18.el7_1.6
libtdb-1.3.8-1.el7_1

141479 - Red Hat Enterprise Linux RHSA-2016-1552 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Description

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

RHSA-2016-1552

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-1552.html>

RHEL6_7S

i386

ntpdate-4.2.6p5-5.el6_7.5
ntp-perl-4.2.6p5-5.el6_7.5
ntp-debuginfo-4.2.6p5-5.el6_7.5
ntp-4.2.6p5-5.el6_7.5

noarch

ntp-doc-4.2.6p5-5.el6_7.5

x86_64

ntpdate-4.2.6p5-5.el6_7.5
ntp-perl-4.2.6p5-5.el6_7.5
ntp-debuginfo-4.2.6p5-5.el6_7.5
ntp-4.2.6p5-5.el6_7.5

141482 - Red Hat Enterprise Linux RHSA-2016-0623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

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

RHSA-2016-0623

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0623.html>

RHEL5_9S

i386

samba-client-3.0.33-3.40.el5_9
samba-debuginfo-3.0.33-3.40.el5_9
libsmbclient-devel-3.0.33-3.40.el5_9
samba-swat-3.0.33-3.40.el5_9
samba-common-3.0.33-3.40.el5_9
libsmbclient-3.0.33-3.40.el5_9
samba-3.0.33-3.40.el5_9

x86_64

samba-client-3.0.33-3.40.el5_9
samba-debuginfo-3.0.33-3.40.el5_9
libsmbclient-devel-3.0.33-3.40.el5_9
samba-swat-3.0.33-3.40.el5_9
samba-common-3.0.33-3.40.el5_9
libsmbclient-3.0.33-3.40.el5_9
samba-3.0.33-3.40.el5_9

RHEL5_6S

i386

samba-client-3.0.33-3.30.el5_6
samba-debuginfo-3.0.33-3.30.el5_6
libsmbclient-3.0.33-3.30.el5_6
samba-swat-3.0.33-3.30.el5_6
samba-common-3.0.33-3.30.el5_6
libsmbclient-devel-3.0.33-3.30.el5_6
samba-3.0.33-3.30.el5_6

x86_64

samba-client-3.0.33-3.30.el5_6
samba-debuginfo-3.0.33-3.30.el5_6
libsmbclient-3.0.33-3.30.el5_6
samba-swat-3.0.33-3.30.el5_6
samba-common-3.0.33-3.30.el5_6
libsmbclient-devel-3.0.33-3.30.el5_6
samba-3.0.33-3.30.el5_6

141487 - Red Hat Enterprise Linux RHSA-2016-0624 Update Is Not Installed

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

Risk Level: Medium

Description

The scan detected that the host is missing the following update:
RHSA-2016-0624

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0624.html>

RHEL5_9S

i386

samba3x-client-3.6.23-12.el5_9
samba3x-winbind-devel-3.6.23-12.el5_9
samba3x-common-3.6.23-12.el5_9
samba3x-3.6.23-12.el5_9
samba3x-winbind-3.6.23-12.el5_9
samba3x-domainjoin-gui-3.6.23-12.el5_9
samba3x-swat-3.6.23-12.el5_9
samba3x-doc-3.6.23-12.el5_9
samba3x-debuginfo-3.6.23-12.el5_9

x86_64

samba3x-client-3.6.23-12.el5_9
samba3x-winbind-devel-3.6.23-12.el5_9
samba3x-common-3.6.23-12.el5_9
samba3x-3.6.23-12.el5_9
samba3x-winbind-3.6.23-12.el5_9
samba3x-domainjoin-gui-3.6.23-12.el5_9
samba3x-swat-3.6.23-12.el5_9
samba3x-doc-3.6.23-12.el5_9
samba3x-debuginfo-3.6.23-12.el5_9

RHEL5_6S

i386

samba3x-winbind-devel-3.6.23-12.el5_6
samba3x-client-3.6.23-12.el5_6
samba3x-doc-3.6.23-12.el5_6
samba3x-common-3.6.23-12.el5_6
samba3x-swat-3.6.23-12.el5_6
samba3x-winbind-3.6.23-12.el5_6
samba3x-debuginfo-3.6.23-12.el5_6
samba3x-3.6.23-12.el5_6
samba3x-domainjoin-gui-3.6.23-12.el5_6

x86_64

samba3x-winbind-devel-3.6.23-12.el5_6
samba3x-client-3.6.23-12.el5_6
samba3x-doc-3.6.23-12.el5_6
samba3x-common-3.6.23-12.el5_6
samba3x-swat-3.6.23-12.el5_6
samba3x-winbind-3.6.23-12.el5_6
samba3x-debuginfo-3.6.23-12.el5_6
samba3x-3.6.23-12.el5_6
samba3x-domainjoin-gui-3.6.23-12.el5_6

141499 - Red Hat Enterprise Linux RHSA-2015-0803 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2596, CVE-2014-5471, CVE-2014-5472, CVE-2014-8159

Description

The scan detected that the host is missing the following update:
RHSA-2015-0803

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-0803.html>

RHEL6_4S

i386

kernel-2.6.32-358.59.1.el6

python-perf-2.6.32-358.59.1.el6

perf-2.6.32-358.59.1.el6

kernel-debuginfo-common-i686-2.6.32-358.59.1.el6

kernel-debug-debuginfo-2.6.32-358.59.1.el6

perf-debuginfo-2.6.32-358.59.1.el6

kernel-debug-2.6.32-358.59.1.el6

kernel-devel-2.6.32-358.59.1.el6

python-perf-debuginfo-2.6.32-358.59.1.el6

kernel-headers-2.6.32-358.59.1.el6

kernel-debuginfo-2.6.32-358.59.1.el6

kernel-debug-devel-2.6.32-358.59.1.el6

noarch

kernel-firmware-2.6.32-358.59.1.el6

kernel-doc-2.6.32-358.59.1.el6

x86_64

kernel-2.6.32-358.59.1.el6

python-perf-2.6.32-358.59.1.el6

perf-2.6.32-358.59.1.el6

kernel-debug-debuginfo-2.6.32-358.59.1.el6

perf-debuginfo-2.6.32-358.59.1.el6

kernel-debug-2.6.32-358.59.1.el6

kernel-debuginfo-common-x86_64-2.6.32-358.59.1.el6

kernel-devel-2.6.32-358.59.1.el6

python-perf-debuginfo-2.6.32-358.59.1.el6

kernel-headers-2.6.32-358.59.1.el6

kernel-debuginfo-2.6.32-358.59.1.el6

kernel-debug-devel-2.6.32-358.59.1.el6

141501 - Red Hat Enterprise Linux RHSA-2015-2587 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2925, CVE-2015-5307, CVE-2015-7613

Description

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

RHSA-2015-2587

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2587.html>

RHEL7_1S

noarch

kernel-doc-3.10.0-229.24.2.el7

kernel-abi-whitelists-3.10.0-229.24.2.el7

x86_64

perf-debuginfo-3.10.0-229.24.2.el7

kernel-debuginfo-common-x86_64-3.10.0-229.24.2.el7

kernel-tools-3.10.0-229.24.2.el7

kernel-debuginfo-3.10.0-229.24.2.el7

kernel-debug-debuginfo-3.10.0-229.24.2.el7

kernel-tools-debuginfo-3.10.0-229.24.2.el7

python-perf-3.10.0-229.24.2.el7

kernel-debug-3.10.0-229.24.2.el7

kernel-devel-3.10.0-229.24.2.el7

kernel-3.10.0-229.24.2.el7

kernel-headers-3.10.0-229.24.2.el7

python-perf-debuginfo-3.10.0-229.24.2.el7

kernel-tools-libs-3.10.0-229.24.2.el7

kernel-tools-libs-devel-3.10.0-229.24.2.el7

perf-3.10.0-229.24.2.el7

kernel-debug-devel-3.10.0-229.24.2.el7

145254 - SuSE SLES 11 SP4 SUSE-SU-2017:0644-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1997

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0644-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002689.html>

SuSE SLES 11 SP4

i586

xorg-x11-libX11-7.4-5.11.68.1

x86_64

xorg-x11-libX11-7.4-5.11.68.1

xorg-x11-libX11-32bit-7.4-5.11.68.1

145255 - SuSE SLES 11 SP4 SUSE-SU-2017:0639-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9913, CVE-2015-7696, CVE-2015-7697, CVE-2016-9844

Description

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

SUSE-SU-2017:0639-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002686.html>

SuSE SLES 11 SP4

i586

unzip-6.00-11.17.1

x86_64

unzip-6.00-11.17.1

185608 - Ubuntu Linux 12.04 USN-3229-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9601, CVE-2016-9189, CVE-2016-9190

Description

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

USN-3229-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003772.html>

Ubuntu 12.04

python-imaging_1.1.7-4ubuntu0.12.04.3

185619 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3230-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9601, CVE-2016-9189, CVE-2016-9190

Description

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

USN-3230-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003774.html>

Ubuntu 16.04

python-imaging_3.1.2-0ubuntu1.1
python-pil_3.1.2-0ubuntu1.1
python3-pil_3.1.2-0ubuntu1.1

Ubuntu 14.04

python3-pil_2.3.0-1ubuntu3.4
python-pil_2.3.0-1ubuntu3.4
python-imaging_2.3.0-1ubuntu3.4
python3-imaging_2.3.0-1ubuntu3.4

Ubuntu 16.10

python-pil_3.3.1-1ubuntu0.1
python-imaging_3.3.1-1ubuntu0.1
python3-pil_3.3.1-1ubuntu0.1

185626 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3222-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10062, CVE-2016-10144, CVE-2016-10145, CVE-2016-10146, CVE-2016-8707, CVE-2017-5506, CVE-2017-5507, CVE-2017-5508, CVE-2017-5510, CVE-2017-5511

Description

The scan detected that the host is missing the following update:
USN-3222-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003765.html>

Ubuntu 12.04

libmagickcore4_6.6.9.7-5ubuntu3.8
imagemagick_6.6.9.7-5ubuntu3.8
libmagickcore4-extra_6.6.9.7-5ubuntu3.8

Ubuntu 16.04

imagemagick_6.8.9.9-7ubuntu5.5
libmagickcore-6.q16-2_6.8.9.9-7ubuntu5.5
libmagickcore-6.q16-2-extra_6.8.9.9-7ubuntu5.5
imagemagick-6.q16_6.8.9.9-7ubuntu5.5

Ubuntu 14.04

libmagickcore5_6.7.7.10-6ubuntu3.5
imagemagick_6.7.7.10-6ubuntu3.5
libmagickcore5-extra_6.7.7.10-6ubuntu3.5

Ubuntu 16.10

libmagickcore-6.q16-2-extra_6.8.9.9-7ubuntu8.4

libmagickcore-6.q16-2_6.8.9.9-7ubuntu8.4

imagemagick-6.q16_6.8.9.9-7ubuntu8.4

imagemagick_6.8.9.9-7ubuntu8.4

191822 - Fedora Linux 25 FEDORA-2017-2e6b693937 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

Description

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

FEDORA-2017-2e6b693937

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

w3m-0.5.3-30.git20170102.fc25

191831 - Fedora Linux 24 FEDORA-2017-3886afeb06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10244

Description

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

FEDORA-2017-3886afeb06

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

freetype-2.6.3-3.fc24

191836 - Fedora Linux 25 FEDORA-2017-c09c0cc384 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10244

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c09c0cc384

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

freetype-2.6.5-3.fc25

141464 - Red Hat Enterprise Linux RHSA-2017-0462 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183

Description

The scan detected that the host is missing the following update:
RHSA-2017-0462

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0462.html>

RHEL7S

x86_64

java-1.8.0-ibm-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.2.el7

RHEL6S

i386

java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.1.el6_8

x86_64

java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.1.el6_8

RHEL6WS

x86_64

java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.1.el6_8

i386

java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.1.el6_8

RHEL7D

x86_64

java-1.8.0-ibm-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.2.el7

RHEL6D

x86_64

java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.1.el6_8

i386

java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.1.el6_8

RHEL7WS

x86_64

java-1.8.0-ibm-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-plugin-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-src-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-jdbc-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-devel-1.8.0.4.1-1jpp.2.el7
java-1.8.0-ibm-demo-1.8.0.4.1-1jpp.2.el7

141467 - Red Hat Enterprise Linux RHSA-2016-1815 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5696

Description

The scan detected that the host is missing the following update:
RHSA-2016-1815

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1815.html>

RHEL6_7S

i386

kernel-devel-2.6.32-573.34.1.el6
python-perf-debuginfo-2.6.32-573.34.1.el6
perf-2.6.32-573.34.1.el6
kernel-debug-2.6.32-573.34.1.el6
kernel-debug-devel-2.6.32-573.34.1.el6
kernel-2.6.32-573.34.1.el6
perf-debuginfo-2.6.32-573.34.1.el6
python-perf-2.6.32-573.34.1.el6
kernel-headers-2.6.32-573.34.1.el6
kernel-debuginfo-common-i686-2.6.32-573.34.1.el6
kernel-debuginfo-2.6.32-573.34.1.el6
kernel-debug-debuginfo-2.6.32-573.34.1.el6

noarch

kernel-doc-2.6.32-573.34.1.el6
kernel-abi-whitelists-2.6.32-573.34.1.el6
kernel-firmware-2.6.32-573.34.1.el6

x86_64

kernel-debug-debuginfo-2.6.32-573.34.1.el6
perf-2.6.32-573.34.1.el6
kernel-debug-devel-2.6.32-573.34.1.el6
kernel-headers-2.6.32-573.34.1.el6
python-perf-2.6.32-573.34.1.el6
kernel-debuginfo-common-i686-2.6.32-573.34.1.el6
kernel-devel-2.6.32-573.34.1.el6
kernel-debuginfo-2.6.32-573.34.1.el6
perf-debuginfo-2.6.32-573.34.1.el6
kernel-2.6.32-573.34.1.el6
python-perf-debuginfo-2.6.32-573.34.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.34.1.el6
kernel-debug-2.6.32-573.34.1.el6

141468 - Red Hat Enterprise Linux RHSA-2016-1207 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7423

Description

The scan detected that the host is missing the following update:
RHSA-2016-1207

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00005.html>

RHEL6_5S

x86_64

glibc-debuginfo-common-2.12-1.132.el6_5.8

glibc-static-2.12-1.132.el6_5.8

glibc-common-2.12-1.132.el6_5.8

glibc-headers-2.12-1.132.el6_5.8

glibc-2.12-1.132.el6_5.8

glibc-debuginfo-2.12-1.132.el6_5.8

glibc-utils-2.12-1.132.el6_5.8

glibc-devel-2.12-1.132.el6_5.8

nscd-2.12-1.132.el6_5.8

191802 - Fedora Linux 24 FEDORA-2017-01eed6fe8c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6232, CVE-2017-6410

Description

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

FEDORA-2017-01eed6fe8c

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

kdelibs3-3.5.10-84.fc24

191813 - Fedora Linux 25 FEDORA-2017-4f4eef4791 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6232, CVE-2017-6410

Description

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

FEDORA-2017-4f4eef4791

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

kdelibs3-3.5.10-84.fc25

130717 - Debian Linux 8.0 DSA-3807-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

Description

The scan detected that the host is missing the following update:
DSA-3807-1

Observation

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

<http://www.debian.org/security/2017/dsa-3807>

Debian 8.0

all

icoutils_0.31.0-2+deb8u3

130719 - Debian Linux 8.0 DSA-3808-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6498, CVE-2017-6499, CVE-2017-6500

Description

The scan detected that the host is missing the following update:
DSA-3808-1

Observation

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

<http://www.debian.org/security/2017/dsa-3808>

Debian 8.0

all

imagemagick_8:6.8.9.9-5+deb8u8

141469 - Red Hat Enterprise Linux RHSA-2016-2076 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4470

Description

The scan detected that the host is missing the following update:
RHSA-2016-2076

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2076.html>

RHEL6_7S

i386

kernel-debug-devel-2.6.32-573.35.1.el6

kernel-debug-2.6.32-573.35.1.el6

perf-debuginfo-2.6.32-573.35.1.el6

python-perf-debuginfo-2.6.32-573.35.1.el6

kernel-debug-debuginfo-2.6.32-573.35.1.el6

kernel-devel-2.6.32-573.35.1.el6

kernel-debuginfo-common-i686-2.6.32-573.35.1.el6

kernel-headers-2.6.32-573.35.1.el6

kernel-debuginfo-2.6.32-573.35.1.el6

kernel-2.6.32-573.35.1.el6

python-perf-2.6.32-573.35.1.el6

perf-2.6.32-573.35.1.el6

noarch

kernel-abi-whitelists-2.6.32-573.35.1.el6

kernel-doc-2.6.32-573.35.1.el6

kernel-firmware-2.6.32-573.35.1.el6

x86_64

perf-2.6.32-573.35.1.el6

kernel-devel-2.6.32-573.35.1.el6

kernel-headers-2.6.32-573.35.1.el6

perf-debuginfo-2.6.32-573.35.1.el6

kernel-2.6.32-573.35.1.el6

kernel-debug-2.6.32-573.35.1.el6

python-perf-debuginfo-2.6.32-573.35.1.el6

kernel-debug-debuginfo-2.6.32-573.35.1.el6

kernel-debuginfo-2.6.32-573.35.1.el6

kernel-debuginfo-common-i686-2.6.32-573.35.1.el6

python-perf-2.6.32-573.35.1.el6

kernel-debuginfo-common-x86_64-2.6.32-573.35.1.el6

kernel-debug-devel-2.6.32-573.35.1.el6

141489 - Red Hat Enterprise Linux RHSA-2016-2694 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7795

Description

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

RHSA-2016-2694

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2694.html>

RHEL7_2S

x86_64

systemd-python-219-19.el7_2.18

systemd-devel-219-19.el7_2.18

systemd-sysv-219-19.el7_2.18

systemd-219-19.el7_2.18
libgudev1-219-19.el7_2.18
systemd-libs-219-19.el7_2.18
systemd-debuginfo-219-19.el7_2.18
systemd-journal-gateway-219-19.el7_2.18
libgudev1-devel-219-19.el7_2.18
systemd-networkd-219-19.el7_2.18
systemd-resolved-219-19.el7_2.18

141491 - Red Hat Enterprise Linux RHSA-2016-0004 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux 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:

RHSA-2016-0004

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0004.html>

RHEL6_4S

i386
kernel-debug-2.6.32-358.69.1.el6
kernel-debug-devel-2.6.32-358.69.1.el6
kernel-devel-2.6.32-358.69.1.el6
python-perf-2.6.32-358.69.1.el6
kernel-debuginfo-common-i686-2.6.32-358.69.1.el6
perf-2.6.32-358.69.1.el6
kernel-debuginfo-2.6.32-358.69.1.el6
kernel-2.6.32-358.69.1.el6
kernel-headers-2.6.32-358.69.1.el6
kernel-debug-debuginfo-2.6.32-358.69.1.el6
perf-debuginfo-2.6.32-358.69.1.el6
python-perf-debuginfo-2.6.32-358.69.1.el6

noarch

kernel-doc-2.6.32-358.69.1.el6
kernel-firmware-2.6.32-358.69.1.el6

x86_64

kernel-debug-2.6.32-358.69.1.el6
kernel-debug-devel-2.6.32-358.69.1.el6
kernel-devel-2.6.32-358.69.1.el6
python-perf-2.6.32-358.69.1.el6
python-perf-debuginfo-2.6.32-358.69.1.el6
perf-2.6.32-358.69.1.el6
kernel-debuginfo-2.6.32-358.69.1.el6
perf-debuginfo-2.6.32-358.69.1.el6
kernel-2.6.32-358.69.1.el6
kernel-headers-2.6.32-358.69.1.el6
kernel-debug-debuginfo-2.6.32-358.69.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.69.1.el6

141493 - Red Hat Enterprise Linux RHSA-2016-1395 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4170

Description

The scan detected that the host is missing the following update:
RHSA-2016-1395

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2016-July/msg00004.html>

RHEL7_1S

noarch

kernel-abi-whitelists-3.10.0-229.38.1.el7

kernel-doc-3.10.0-229.38.1.el7

x86_64

kernel-tools-3.10.0-229.38.1.el7

kernel-tools-libs-devel-3.10.0-229.38.1.el7

kernel-tools-debuginfo-3.10.0-229.38.1.el7

kernel-devel-3.10.0-229.38.1.el7

kernel-debug-debuginfo-3.10.0-229.38.1.el7

kernel-debug-devel-3.10.0-229.38.1.el7

kernel-headers-3.10.0-229.38.1.el7

kernel-debuginfo-common-x86_64-3.10.0-229.38.1.el7

kernel-debug-3.10.0-229.38.1.el7

kernel-debuginfo-3.10.0-229.38.1.el7

perf-debuginfo-3.10.0-229.38.1.el7

python-perf-3.10.0-229.38.1.el7

kernel-3.10.0-229.38.1.el7

kernel-tools-libs-3.10.0-229.38.1.el7

perf-3.10.0-229.38.1.el7

python-perf-debuginfo-3.10.0-229.38.1.el7

141494 - Red Hat Enterprise Linux RHSA-2016-2074 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4470

Description

The scan detected that the host is missing the following update:
RHSA-2016-2074

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2074.html>

RHEL6_5S

x86_64
python-perf-2.6.32-431.74.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.74.1.el6
kernel-debuginfo-2.6.32-431.74.1.el6
kernel-debug-devel-2.6.32-431.74.1.el6
perf-2.6.32-431.74.1.el6
perf-debuginfo-2.6.32-431.74.1.el6
kernel-headers-2.6.32-431.74.1.el6
python-perf-debuginfo-2.6.32-431.74.1.el6
kernel-debug-debuginfo-2.6.32-431.74.1.el6
kernel-2.6.32-431.74.1.el6
kernel-debug-2.6.32-431.74.1.el6
kernel-devel-2.6.32-431.74.1.el6

noarch
kernel-firmware-2.6.32-431.74.1.el6
kernel-doc-2.6.32-431.74.1.el6
kernel-abi-whitelists-2.6.32-431.74.1.el6

141497 - Red Hat Enterprise Linux RHSA-2015-2645 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux 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:
RHSA-2015-2645

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2645.html>

RHEL6_5S
i386
kernel-debug-2.6.32-431.68.1.el6
kernel-2.6.32-431.68.1.el6
python-perf-debuginfo-2.6.32-431.68.1.el6
kernel-debug-debuginfo-2.6.32-431.68.1.el6
perf-debuginfo-2.6.32-431.68.1.el6
kernel-debuginfo-2.6.32-431.68.1.el6
kernel-headers-2.6.32-431.68.1.el6
kernel-debuginfo-common-i686-2.6.32-431.68.1.el6
kernel-devel-2.6.32-431.68.1.el6
python-perf-2.6.32-431.68.1.el6
kernel-debug-devel-2.6.32-431.68.1.el6
perf-2.6.32-431.68.1.el6

noarch
kernel-doc-2.6.32-431.68.1.el6
kernel-abi-whitelists-2.6.32-431.68.1.el6
kernel-firmware-2.6.32-431.68.1.el6

x86_64
kernel-debug-2.6.32-431.68.1.el6
kernel-2.6.32-431.68.1.el6

python-perf-debuginfo-2.6.32-431.68.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.68.1.el6
kernel-debug-debuginfo-2.6.32-431.68.1.el6
perf-debuginfo-2.6.32-431.68.1.el6
kernel-debuginfo-2.6.32-431.68.1.el6
kernel-headers-2.6.32-431.68.1.el6
kernel-devel-2.6.32-431.68.1.el6
python-perf-2.6.32-431.68.1.el6
kernel-debug-devel-2.6.32-431.68.1.el6
perf-2.6.32-431.68.1.el6

141504 - Red Hat Enterprise Linux RHSA-2015-1643 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3636

Description

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

RHSA-2015-1643

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2015-1643.html>

RHEL6_4S

i386
kernel-2.6.32-358.65.1.el6
kernel-headers-2.6.32-358.65.1.el6
kernel-debug-debuginfo-2.6.32-358.65.1.el6
perf-2.6.32-358.65.1.el6
perf-debuginfo-2.6.32-358.65.1.el6
kernel-debug-2.6.32-358.65.1.el6
python-perf-2.6.32-358.65.1.el6
kernel-debug-devel-2.6.32-358.65.1.el6
kernel-devel-2.6.32-358.65.1.el6
kernel-debuginfo-common-i686-2.6.32-358.65.1.el6
kernel-debuginfo-2.6.32-358.65.1.el6
python-perf-debuginfo-2.6.32-358.65.1.el6

noarch

kernel-firmware-2.6.32-358.65.1.el6
kernel-doc-2.6.32-358.65.1.el6

x86_64

python-perf-2.6.32-358.65.1.el6
kernel-2.6.32-358.65.1.el6
kernel-headers-2.6.32-358.65.1.el6
kernel-debug-debuginfo-2.6.32-358.65.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.65.1.el6
perf-debuginfo-2.6.32-358.65.1.el6
kernel-debug-2.6.32-358.65.1.el6
perf-2.6.32-358.65.1.el6
kernel-debug-devel-2.6.32-358.65.1.el6
kernel-devel-2.6.32-358.65.1.el6
kernel-debuginfo-2.6.32-358.65.1.el6

145251 - SuSE SLES 11 SP4 SUSE-SU-2017:0647-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8106, CVE-2016-10155, CVE-2016-9101, CVE-2016-9776, CVE-2016-9907, CVE-2016-9911, CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620, CVE-2017-5579, CVE-2017-5856, CVE-2017-5898, CVE-2017-5973

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0647-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002690.html>

SuSE SLES 11 SP4

x86_64

xen-kmp-default-4.4.4_14_3.0.101_94-51.1

xen-tools-domU-4.4.4_14-51.1

xen-4.4.4_14-51.1

xen-libs-4.4.4_14-51.1

xen-tools-4.4.4_14-51.1

xen-libs-32bit-4.4.4_14-51.1

xen-doc-html-4.4.4_14-51.1

i586

xen-kmp-default-4.4.4_14_3.0.101_94-51.1

xen-tools-domU-4.4.4_14-51.1

xen-kmp-pae-4.4.4_14_3.0.101_94-51.1

xen-libs-4.4.4_14-51.1

182300 - FreeBSD kde-runtime Kdesu: Displayed Command Truncated By Unicode String Terminator (41fe4724-06a2-11e7-8e3e-5453ed2e2b49)

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

Risk Level: Medium

CVE: CVE-2016-7787

Description

The scan detected that the host is missing the following update:
kde-runtime -- kdesu: displayed command truncated by unicode string terminator (41fe4724-06a2-11e7-8e3e-5453ed2e2b49)

Observation

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

<http://www.vuxml.org/freebsd/41fe4724-06a2-11e7-8e3e-5453ed2e2b49.html>

Affected packages:

kde-runtime < 4.14.3_5

185609 - Ubuntu Linux 12.04, 14.04 USN-3223-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6410

Description

The scan detected that the host is missing the following update:
USN-3223-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003767.html>

Ubuntu 12.04

kdelibs5-plugins_4.8.5-0ubuntu0.6

Ubuntu 14.04

kdelibs5-plugins_4.13.3-0ubuntu0.4

185617 - Ubuntu Linux 12.04 USN-3226-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

Description

The scan detected that the host is missing the following update:
USN-3226-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003770.html>

Ubuntu 12.04

icoutils_0.29.1-2ubuntu0.2

185624 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3232-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6498, CVE-2017-6499, CVE-2017-6500

Description

The scan detected that the host is missing the following update:
USN-3232-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003776.html>

Ubuntu 12.04

imagemagick_6.6.9.7-5ubuntu3.9
libmagickcore4_6.6.9.7-5ubuntu3.9
libmagickcore4-extra_6.6.9.7-5ubuntu3.9

Ubuntu 16.04

libmagickcore-6.q16-2-extra_6.8.9.9-7ubuntu5.6
imagemagick_6.8.9.9-7ubuntu5.6
libmagickcore-6.q16-2_6.8.9.9-7ubuntu5.6
imagemagick-6.q16_6.8.9.9-7ubuntu5.6

Ubuntu 14.04

libmagickcore5_6.7.7.10-6ubuntu3.6
libmagickcore5-extra_6.7.7.10-6ubuntu3.6
imagemagick_6.7.7.10-6ubuntu3.6

Ubuntu 16.10

libmagickcore-6.q16-2-extra_6.8.9.9-7ubuntu8.5
libmagickcore-6.q16-2_6.8.9.9-7ubuntu8.5
imagemagick-6.q16_6.8.9.9-7ubuntu8.5
imagemagick_6.8.9.9-7ubuntu8.5

191824 - Fedora Linux 24 FEDORA-2017-b011e8c922 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6410

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b011e8c922

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

kdelibs-4.14.29-2.fc24

33365 - Oracle Solaris 152644-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152644-03

Observation

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

<https://getupdates.oracle.com/readme/152644-03>

SunOS 5.10(x86): Apache 2.4 Patch

SOLARIS_10_x86

SUNWapch2r:11.10.0,REV=2005.01.08.01.09

SUNWapch2d:11.10.0,REV=2005.01.08.01.09

SUNWapch2S:11.10.0,REV=2005.01.08.01.09

SUNWapch2u:11.10.0,REV=2005.01.08.01.09

33366 - Oracle Solaris 152643-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152643-03

Observation

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

<https://getupdates.oracle.com/readme/152643-03>

SunOS 5.10: Apache 2.4 Patch

SOLARIS_10

SUNWapch2d:11.10.0,REV=2005.01.08.05.16

SUNWapch2S:11.10.0,REV=2005.01.08.05.16

SUNWapch2u:11.10.0,REV=2005.01.08.05.16

SUNWapch2r:11.10.0,REV=2005.01.08.05.16

88849 - Slackware Linux 14.1, 14.2 SSA:2017-066-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2017-066-01

Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.398307>

Slackware 14.1

x86_64

mozilla-firefox-45.8.0esr-x86_64-1

Slackware 14.2

x86_64

mozilla-firefox-45.8.0esr-x86_64-1

i586

mozilla-firefox-45.8.0esr-i586-1

88850 - Slackware Linux 14.1, 14.2 SSA:2017-066-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

SSA:2017-066-02

Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.403003>

Slackware 14.1

x86_64

mozilla-thunderbird-45.8.0-x86_64-1

Slackware 14.2

x86_64

mozilla-thunderbird-45.8.0-x86_64-1

i586

mozilla-thunderbird-45.8.0-i586-1

130716 - Debian Linux 8.0 DSA-3805-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

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

DSA-3805-1

Observation

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

<http://www.debian.org/security/2017/dsa-3805>

Debian 8.0
all
firefox-esr_45.8.0esr-1~deb8u1

130718 - Debian Linux 8.0 DSA-3803-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10243

Description

The scan detected that the host is missing the following update:
DSA-3803-1

Observation

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

<http://www.debian.org/security/2017/dsa-3803>

Debian 8.0
all
texlive-base_2014.20141024-2+deb8u1

130721 - Debian Linux 8.0 DSA-3806-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2640

Description

The scan detected that the host is missing the following update:
DSA-3806-1

Observation

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

<http://www.debian.org/security/2017/dsa-3806>

Debian 8.0
all
pidgin_2.11.0-0+deb8u2

141480 - Red Hat Enterprise Linux RHSA-2016-0559 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2016-0559

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0559.html>

RHEL5_6S

i386

redhat-release-5Server-5.6.0.10

x86_64

redhat-release-5Server-5.6.0.10

141481 - Red Hat Enterprise Linux RHSA-2016-1991 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2016-1991

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1991.html>

RHEL5_6S

i386

redhat-release-5Server-5.6.0.11

x86_64

redhat-release-5Server-5.6.0.11

141485 - Red Hat Enterprise Linux RHSA-2016-2008 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2016-2008

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2008.html>

RHEL7_1S
x86_64
redhat-release-server-7.1-1.el7_1.4

141490 - Red Hat Enterprise Linux RHSA-2016-2998 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2016-2998

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2998.html>

RHEL6_2S
x86_64
redhat-release-server-6Server-6.2.0.7.el6_2

182299 - FreeBSD chromium Multiple Vulnerabilities (a505d397-0758-11e7-8d8b-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5032, CVE-2017-5033, CVE-2017-5034, CVE-2017-5035, CVE-2017-5036, CVE-2017-5037, CVE-2017-5038, CVE-2017-5039, CVE-2017-5040, CVE-2017-5041, CVE-2017-5042, CVE-2017-5043, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (a505d397-0758-11e7-8d8b-e8e0b747a45a)

Observation

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

<http://www.vuxml.org/freebsd/a505d397-0758-11e7-8d8b-e8e0b747a45a.html>

Affected packages:
chromium < 57.0.2987.98
chromium-npapi < 57.0.2987.98
chromium-pulse < 57.0.2987.98

182301 - FreeBSD wordpress Multiple Vulnerabilities (82752070-0349-11e7-b48d-00e04c1ea73d)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
wordpress -- multiple vulnerabilities (82752070-0349-11e7-b48d-00e04c1ea73d)

Observation

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

<http://www.vuxml.org/freebsd/82752070-0349-11e7-b48d-00e04c1ea73d.html>

Affected packages:

wordpress < 4.7.3,1
de-wordpress < 4.7.3
ja-wordpress < 4.7.3
ru-wordpress < 4.7.3
zh-wordpress-zh_CN < 4.7.3
zh-wordpress-zh_TW < 4.7.3

182302 - FreeBSD Several Security Defects In The Bouncy Castle Crypto APIs (89cf8cd2-0698-11e7-aa3f-001b216d295b)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
Several Security Defects in the Bouncy Castle Crypto APIs (89cf8cd2-0698-11e7-aa3f-001b216d295b)

Observation

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

<http://www.vuxml.org/freebsd/89cf8cd2-0698-11e7-aa3f-001b216d295b.html>

Affected packages:

1.51 <= bouncycastle15 < 1.56

182303 - FreeBSD kdepimlibs Directory Traversal On KTNEF (e550fc62-069a-11e7-8e3e-5453ed2e2b49)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
kdepimlibs -- directory traversal on KTNEF (e550fc62-069a-11e7-8e3e-5453ed2e2b49)

Observation

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

<http://www.vuxml.org/freebsd/e550fc62-069a-11e7-8e3e-5453ed2e2b49.html>

Affected packages:

kdepimlibs < 4.14.10_7

182304 - FreeBSD Kio: Information Leak When Accessing Https When Using A Malicious PAC File (f714d8ab-028e-11e7-8042-50e549ebab6c)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

kio: Information Leak when accessing https when using a malicious PAC file (f714d8ab-028e-11e7-8042-50e549ebab6c)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/f714d8ab-028e-11e7-8042-50e549ebab6c.html>

Affected packages:

kdelibs < 4.14.29_10

kf5-kio < 5.31.0_1

182305 - FreeBSD mbed TLS (PolarSSL) Multiple Vulnerabilities (f41e3e54-076b-11e7-a9f2-0011d823eebd)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

mbed TLS (PolarSSL) -- multiple vulnerabilities (f41e3e54-076b-11e7-a9f2-0011d823eebd)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/f41e3e54-076b-11e7-a9f2-0011d823eebd.html>

Affected packages:

mbedtls < 2.4.2

polarssl13 < 1.3.19

185613 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3224-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5985

Description

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

USN-3224-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003768.html>

Ubuntu 16.04

lxc-common_2.0.7-0ubuntu1~16.04.2

Ubuntu 14.04

lxc_1.0.9-0ubuntu3

Ubuntu 16.10

lxc-common_2.0.7-0ubuntu1~16.10.2

185622 - Ubuntu Linux 12.04, 14.04 USN-3231-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2640

Description

The scan detected that the host is missing the following update:
USN-3231-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003775.html>

Ubuntu 12.04

libpurple0_2.10.3-0ubuntu1.8

Ubuntu 14.04

libpurple0_2.10.9-0ubuntu3.4

185625 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3228-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Description

The scan detected that the host is missing the following update:
USN-3228-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003773.html>

Ubuntu 12.04

libevent-2.0-5_2.0.16-stable-1ubuntu0.2

Ubuntu 16.04

libevent-2.0-5_2.0.21-stable-2ubuntu0.16.04.1

Ubuntu 14.04

libevent-2.0-5_2.0.21-stable-1ubuntu1.14.04.2

Ubuntu 16.10

libevent-2.0-5_2.0.21-stable-2ubuntu0.16.10.1

191800 - Fedora Linux 25 FEDORA-2017-bb459964ce 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-2017-bb459964ce

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

firefox-52.0-1.fc25

191803 - Fedora Linux 25 FEDORA-2017-ca3f01bd37 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-2017-ca3f01bd37

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

php-pear-PHP-CodeSniffer-2.8.1-1.fc25

191804 - Fedora Linux 25 FEDORA-2017-884de1e698 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-2017-884de1e698

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

deluge-1.3.14-1.fc25

191805 - Fedora Linux 24 FEDORA-2017-e63f2f0d11 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-2017-e63f2f0d11

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

thunderbird-45.8.0-1.fc24

191807 - Fedora Linux 25 FEDORA-2017-038e821698 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-2017-038e821698

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

knot-2.4.1-1.fc25

knot-resolver-1.2.3-1.fc25

191810 - Fedora Linux 25 FEDORA-2017-c87bbae385 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-2017-c87bbae385

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

drupal7-metatag-1.21-1.fc25

191812 - Fedora Linux 24 FEDORA-2017-aaf92c483c 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-2017-aaf92c483c

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

php-pear-PHP-CodeSniffer-2.8.1-1.fc24

191814 - Fedora Linux 24 FEDORA-2017-f3484d64d2 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-2017-f3484d64d2

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

firefox-52.0-1.fc24

191817 - Fedora Linux 24 FEDORA-2017-5b32a5782b 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-2017-5b32a5782b

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

tor-0.2.9.10-1.fc24

191819 - Fedora Linux 25 FEDORA-2017-fce0c6fd46 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-2017-fce0c6fd46

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

thunderbird-45.8.0-1.fc25

191821 - Fedora Linux 25 FEDORA-2017-06365bdcfd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6430

Description

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

FEDORA-2017-06365bdcfd

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

ettercap-0.8.2-4.1.fc25

191823 - Fedora Linux 25 FEDORA-2017-6f3ea63acc 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-2017-6f3ea63acc

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

tor-0.2.9.10-1.fc25

191825 - Fedora Linux 24 FEDORA-2017-bcab179007 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-2017-bcab179007

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

drupal7-views-3.15-1.fc24

191826 - Fedora Linux 25 FEDORA-2017-82ce4661d6 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-2017-82ce4661d6

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

drupal7-views-3.15-1.fc25

191829 - Fedora Linux 24 FEDORA-2017-1607a3a78e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2620

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1607a3a78e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

xen-4.6.4-8.fc24

191830 - Fedora Linux 25 FEDORA-2017-f3aac83a8f 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-2017-f3aac83a8f

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

suricata-3.2.1-1.fc25

191832 - Fedora Linux 24 FEDORA-2017-cc7249b821 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-2017-cc7249b821

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

drupal7-metatag-1.21-1.fc24

191833 - Fedora Linux 25 FEDORA-2017-98f85533f0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2590

Description

The scan detected that the host is missing the following update:
FEDORA-2017-98f85533f0

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

freeipa-4.4.3-2.fc25

191834 - Fedora Linux 24 FEDORA-2017-f9f3a78148 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-2017-f9f3a78148

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

suricata-3.2.1-1.fc24

191837 - Fedora Linux 24 FEDORA-2017-a513be0939 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4000

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a513be0939

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

cacti-1.0.4-1.fc24

191820 - Fedora Linux 24 FEDORA-2017-25df1dbd02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6188

Description

The scan detected that the host is missing the following update:
FEDORA-2017-25df1dbd02

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

munin-2.0.30-5.fc24

191828 - Fedora Linux 25 FEDORA-2017-3776c9d747 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6188

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3776c9d747

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

munin-2.0.30-5.fc25

21330 - Microsoft Office 2016 Click-To-Run March 2017 Updates

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run.

Observation

Microsoft Office 2016 Click-to-Run is an alternative to the Windows Installer-based (MSI) installation method of the popular office suite.

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

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.

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

20140 - (MS16-077) Security Update for WPAD (3165191)

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

Risk Level: High

CVE: CVE-2016-3213, CVE-2016-3236

Update Details

Recommendation is updated

20640 - (MS16-123) Security Update for Windows Kernel-Mode Drivers (3192892)

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

Risk Level: High

CVE: CVE-2016-3266, CVE-2016-3341, CVE-2016-3376, CVE-2016-7185, CVE-2016-7211

Update Details

Recommendation is updated

20645 - (MS16-123) Microsoft Windows Win32k Privilege Escalation I (3192892)

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

Risk Level: High

CVE: CVE-2016-3266

Update Details

Recommendation is updated

20678 - (MS16-120) Security Update for Microsoft Graphics Component (3192884)

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

Risk Level: High

CVE: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182

Update Details

Recommendation is updated

20679 - (MS16-120) Security Update for Microsoft Graphics Component (3192884)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182

Update Details

Recommendation is updated

20680 - (MS16-120) Microsoft Windows Graphics Win32k Privilege Escalation (3192884)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3270

[Update Details](#)

Recommendation is updated

20681 - (MS16-120) Microsoft Windows Graphics True Type Font Parsing Privilege Escalation (3192884)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-7182

[Update Details](#)

Recommendation is updated

21501 - (APSB17-07) Vulnerabilities In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003

[Update Details](#)

Risk is updated

21503 - (APSB17-07) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003

[Update Details](#)

Risk is updated

140676 - Red Hat Enterprise Linux RHSA-2015-0140 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0314, CVE-2015-0315, CVE-2015-0316, CVE-2015-0317, CVE-2015-0318, CVE-2015-0319, CVE-2015-0320, CVE-2015-0321, CVE-2015-0322, CVE-2015-0323, CVE-2015-0324, CVE-2015-0325, CVE-2015-0326, CVE-2015-0327, CVE-2015-0328, CVE-2015-0329, CVE-2015-0330, CVE-2015-0331

[Update Details](#)

CVE is updated

140916 - Red Hat Enterprise Linux RHSA-2015-1603 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5127, CVE-2015-5129, CVE-2015-5130, CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-5557, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, CVE-2015-5563, CVE-2015-5564, CVE-2015-5565, CVE-2015-5566

[Update Details](#)

CVE is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

141035 - Red Hat Enterprise Linux RHSA-2015-2593 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8454, CVE-2015-8455, CVE-2015-8456, CVE-2015-8457, CVE-2015-8652, CVE-2015-8653, CVE-2015-8654, CVE-2015-8655, CVE-2015-8656, CVE-2015-8657, CVE-2015-8658, CVE-2015-8820, CVE-2015-8821, CVE-2015-8822, CVE-2015-8823

[Update Details](#)

CVE is updated

141042 - Red Hat Enterprise Linux RHSA-2015-2657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

[Update Details](#)

FASLScript is updated

141049 - Red Hat Enterprise Linux RHSA-2015-2697 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651, CVE-2016-0959

[Update Details](#)

CVE is updated

141050 - Red Hat Enterprise Linux RHSA-2016-0001 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214

[Update Details](#)

FASLScript is updated

141075 - Red Hat Enterprise Linux RHSA-2016-0071 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1930, CVE-2016-1935

[Update Details](#)

FASLScript is updated

141096 - Red Hat Enterprise Linux RHSA-2016-0258 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1521, CVE-2016-1522, CVE-2016-1523, CVE-2016-1930, CVE-2016-1935

[Update Details](#)

FASLScript is updated

141103 - Red Hat Enterprise Linux RHSA-2016-0301 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3197, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0800

[Update Details](#)

FASLScript is updated

141116 - Red Hat Enterprise Linux RHSA-2016-0373 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1952, CVE-2016-1954, CVE-2016-1957, CVE-2016-1958, CVE-2016-1960, CVE-2016-1961, CVE-2016-1962, CVE-2016-1964, CVE-2016-1965, CVE-2016-1966, CVE-2016-1973, CVE-2016-1974, CVE-2016-1977, CVE-2016-2790, CVE-2016-2791, CVE-2016-2792, CVE-2016-2793, CVE-2016-2794, CVE-2016-2795, CVE-2016-2796, CVE-2016-2797, CVE-2016-2798, CVE-2016-2799, CVE-2016-2800, CVE-2016-2801, CVE-2016-2802

[Update Details](#)

FASLScript is updated

141133 - Red Hat Enterprise Linux RHSA-2016-0496 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2315, CVE-2016-2324

[Update Details](#)

FASLScript is updated

141137 - Red Hat Enterprise Linux RHSA-2016-0497 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2315, CVE-2016-2324

[Update Details](#)

FASLScript is updated

141166 - Red Hat Enterprise Linux RHSA-2016-0695 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1526, CVE-2016-2805, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

[Update Details](#)

CVE is updated FASLScript is updated

141167 - Red Hat Enterprise Linux RHSA-2016-0676 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

[Update Details](#)

FASLScript is updated

141169 - Red Hat Enterprise Linux RHSA-2016-0650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

[Update Details](#)

FASLScript is updated

141172 - Red Hat Enterprise Linux RHSA-2016-0716 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3009, CVE-2013-5456, CVE-2016-0264, CVE-2016-0363, CVE-2016-0376, CVE-2016-0686, CVE-2016-0687, CVE-2016-3422, CVE-2016-3426, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

[Update Details](#)

FASLScript is updated

141175 - Red Hat Enterprise Linux RHSA-2016-0701 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3009, CVE-2013-5456, CVE-2016-0264, CVE-2016-0363, CVE-2016-0376, CVE-2016-0686, CVE-2016-0687, CVE-2016-3422, CVE-2016-3426, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

[Update Details](#)

FASLScript is updated

141176 - Red Hat Enterprise Linux RHSA-2016-0705 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4792, CVE-2015-4800, CVE-2015-4802, CVE-2015-4815, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4862, CVE-2015-4870, CVE-2015-4890, CVE-2015-4910, CVE-2015-4913, CVE-2016-0503, CVE-2016-0504, CVE-2016-0505, CVE-2016-0546, CVE-2016-0595, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0605, CVE-2016-0606, CVE-2016-0607, CVE-2016-0608, CVE-2016-0609, CVE-2016-0610, CVE-2016-0611, CVE-2016-0639, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0655, CVE-2016-0661, CVE-2016-0665, CVE-2016-0666, CVE-2016-0668, CVE-2016-2047, CVE-2016-3452, CVE-2016-3471, CVE-2016-5444

[Update Details](#)

CVE is updated FASLScript is updated

141179 - Red Hat Enterprise Linux RHSA-2016-0722 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

[Update Details](#)

FASLScript is updated

141180 - Red Hat Enterprise Linux RHSA-2016-0726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

[Update Details](#)

FASLScript is updated

141192 - Red Hat Enterprise Linux RHSA-2016-1041 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2807

[Update Details](#)

FASLScript is updated

141213 - Red Hat Enterprise Linux RHSA-2016-1237 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8895, CVE-2015-8896, CVE-2015-8897, CVE-2015-8898, CVE-2016-5118, CVE-2016-5239, CVE-2016-5240

[Update Details](#)

FASLScript is updated

141214 - Red Hat Enterprise Linux RHSA-2016-1292 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449

[Update Details](#)

FASLScript is updated

141240 - Red Hat Enterprise Linux RHSA-2016-1582 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000, CVE-2016-1000023

[Update Details](#)

FASLScript is updated

141245 - Red Hat Enterprise Linux RHSA-2016-1583 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000, CVE-2016-1000023

[Update Details](#)

FASLScript is updated

141313 - Red Hat Enterprise Linux RHSA-2016-2131 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

FASLScript is updated

141316 - Red Hat Enterprise Linux RHSA-2016-2130 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283

[Update Details](#)

FASLScript is updated

141322 - Red Hat Enterprise Linux RHSA-2016-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

FASLScript is updated

141331 - Red Hat Enterprise Linux RHSA-2016-2574 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2015-8956, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3044, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-3841, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2016-7914, CVE-2016-7915, CVE-2016-9794

[Update Details](#)

CVE is updated FASLScript is updated

141349 - Red Hat Enterprise Linux RHSA-2016-2586 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5636

[Update Details](#)

FASLScript is updated

141361 - Red Hat Enterprise Linux RHSA-2016-2750 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7456, CVE-2014-9767, CVE-2015-2325, CVE-2015-2326, CVE-2015-2327, CVE-2015-2328, CVE-2015-3210, CVE-2015-3217, CVE-2015-5073, CVE-2015-8381, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8388, CVE-2015-8391, CVE-2015-8392, CVE-2015-8395, CVE-2015-8835, CVE-2015-8865, CVE-2015-8866, CVE-2015-8867, CVE-2015-8873, CVE-2015-8874, CVE-2015-8876, CVE-2015-8877, CVE-2015-8879, CVE-2016-1903, CVE-2016-2554, CVE-2016-3074, CVE-2016-3141, CVE-2016-3142, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4342, CVE-2016-4343, CVE-2016-4473, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544, CVE-2016-5093, CVE-2016-5094, CVE-2016-5096, CVE-2016-5114, CVE-2016-5399, CVE-2016-5766, CVE-2016-5767, CVE-2016-5768, CVE-2016-5770, CVE-2016-5771, CVE-2016-5772, CVE-2016-5773, CVE-2016-6128, CVE-2016-6207, CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297, CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132

[Update Details](#)

FASLScript is updated

141364 - Red Hat Enterprise Linux RHSA-2016-2749 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283

[Update Details](#)

FASLScript is updated

141379 - Red Hat Enterprise Linux RHSA-2016-2928 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

FASLScript is updated

141380 - Red Hat Enterprise Linux RHSA-2016-2927 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-5630, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

FASLScript 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

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

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

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

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, CVE-2016-3679

[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

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

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

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

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

19353 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3116180)

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

Risk Level: High
CVE: CVE-2015-6083

[Update Details](#)

Recommendation is updated

19354 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3116180)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6134

[Update Details](#)

Recommendation is updated

19356 - (MS15-124) Microsoft Internet Explorer Script Engine Memory Corruption Remote Code Execution (3116180)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6136

[Update Details](#)

Recommendation is updated

19359 - (MS15-124) Microsoft Internet Explorer Browser Content Privilege Escalation (3116180)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6139

[Update Details](#)

Recommendation is updated

19360 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3116180)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6140

[Update Details](#)

Recommendation is updated

19361 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3116180)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6141

[Update Details](#)

Recommendation is updated

19362 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3116180)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6142

[Update Details](#)

Recommendation is updated

19363 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3116180)

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

Risk Level: High

CVE: CVE-2015-6143

[Update Details](#)

Recommendation is updated

19365 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3116180)

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

Risk Level: High

CVE: CVE-2015-6145

[Update Details](#)

Recommendation is updated

19366 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3116180)

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

Risk Level: High

CVE: CVE-2015-6146

[Update Details](#)

Recommendation is updated

19367 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3116180)

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

Risk Level: High

CVE: CVE-2015-6147

[Update Details](#)

Recommendation is updated

19368 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3116180)

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

Risk Level: High

CVE: CVE-2015-6148

[Update Details](#)

Recommendation is updated

19369 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3116180)

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

Risk Level: High

CVE: CVE-2015-6149

[Update Details](#)

Recommendation is updated

19370 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3116180)

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

Risk Level: High

CVE: CVE-2015-6150

[Update Details](#)

Recommendation is updated

19371 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3116180)

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

Risk Level: High

CVE: CVE-2015-6151

[Update Details](#)

Recommendation is updated

19372 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3116180)

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

Risk Level: High

CVE: CVE-2015-6152

[Update Details](#)

Recommendation is updated

19373 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XV (3116180)

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

Risk Level: High

CVE: CVE-2015-6153

[Update Details](#)

Recommendation is updated

19374 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVI (3116180)

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

Risk Level: High

CVE: CVE-2015-6154

[Update Details](#)

Recommendation is updated

19375 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVII (3116180)

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

Risk Level: High

CVE: CVE-2015-6155

[Update Details](#)

Recommendation is updated

19376 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVIII (3116180)

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

Risk Level: High

CVE: CVE-2015-6156

[Update Details](#)

Recommendation is updated

19378 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIX (3116180)

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

Risk Level: High

CVE: CVE-2015-6158

[Update Details](#)

Recommendation is updated

19379 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XX (3116180)

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

Risk Level: High

CVE: CVE-2015-6159

[Update Details](#)

Recommendation is updated

19380 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXI (3116180)

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

Risk Level: High

CVE: CVE-2015-6160

Update Details

Recommendation is updated

19382 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXII (3116180)

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

Risk Level: High

CVE: CVE-2015-6162

Update Details

Recommendation is updated

19397 - (MS15-124) Cumulative Security Update for Internet Explorer (3116180)

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

Risk Level: High

CVE: CVE-2015-6083, CVE-2015-6134, CVE-2015-6135, CVE-2015-6136, CVE-2015-6138, CVE-2015-6139, CVE-2015-6140, CVE-2015-6141, CVE-2015-6142, CVE-2015-6143, CVE-2015-6144, CVE-2015-6145, CVE-2015-6146, CVE-2015-6147, CVE-2015-6148, CVE-2015-6149, CVE-2015-6150, CVE-2015-6151, CVE-2015-6152, CVE-2015-6153, CVE-2015-6154, CVE-2015-6155, CVE-2015-6156, CVE-2015-6157, CVE-2015-6158, CVE-2015-6159, CVE-2015-6160, CVE-2015-6161, CVE-2015-6162, CVE-2015-6164

Update Details

Recommendation is updated

19523 - (MS16-001) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution (3124903)

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

Risk Level: High

CVE: CVE-2016-0002

Update Details

Recommendation is updated

19531 - (MS16-001) Cumulative Security Update for Internet Explorer (3124903)

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

Risk Level: High

CVE: CVE-2016-0002, CVE-2016-0005

Update Details

Recommendation is updated

20006 - (MS16-061) Security Update for Microsoft RPC (3155520)

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

Risk Level: High

CVE: CVE-2016-0178

Update Details

Recommendation is updated

20008 - (MS16-061) Microsoft Windows Remote Procedure Call NDR Engine Privilege Escalation (3155520)

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

Risk Level: High

CVE: CVE-2016-0178

Update Details

Recommendation is updated

20051 - (MS16-056) Microsoft Windows Journal Memory Corruption Remote Code Execution (3156761)

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

Risk Level: High

CVE: CVE-2016-0182

Update Details

Recommendation is updated

20052 - (MS16-056) Security Update for Windows Journal (3156761)

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

Risk Level: High

CVE: CVE-2016-0182

Update Details

Recommendation is updated

20056 - (MS16-057) Microsoft Windows Shell Remote Code Execution (3156987)

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

Risk Level: High

CVE: CVE-2016-0179

Update Details

Recommendation is updated

20057 - (MS16-057) Security Update for Windows Shell (3156987)

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

Risk Level: High

CVE: CVE-2016-0179

Update Details

Recommendation is updated

20150 - (MS16-068) Microsoft Edge Chakra Scripting Engine Memory Corruption Remote Code Execution I (3163656)

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

Risk Level: High

CVE: CVE-2016-3199

Update Details

Recommendation is updated

20153 - (MS16-068) Microsoft Edge PDF Remote Code Execution (3163656)

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

Risk Level: High

CVE: CVE-2016-3203

Update Details

Recommendation is updated

20154 - (MS16-068) Microsoft Edge Chakra Scripting Engine Memory Corruption Remote Code Execution III (3163656)

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

Risk Level: High

CVE: CVE-2016-3214

Update Details

Recommendation is updated

20157 - (MS16-068) Cumulative Security Update for Microsoft Edge (3163656)

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

Risk Level: High

CVE: CVE-2016-3198, CVE-2016-3199, CVE-2016-3201, CVE-2016-3202, CVE-2016-3203, CVE-2016-3214, CVE-2016-3215, CVE-2016-3222

Update Details

Recommendation is updated

20273 - (MS16-087) Microsoft Windows Print Spooler Drivers Remote Code Execution (3170005)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3238

[Update Details](#)

Recommendation is updated

20279 - (MS16-087) Security Update for Windows Print Spooler Components (3170005)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3238, CVE-2016-3239

[Update Details](#)

Recommendation is updated

20295 - (MS16-085) Cumulative Security Update for Microsoft Edge (3169999)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3244, CVE-2016-3246, CVE-2016-3248, CVE-2016-3259, CVE-2016-3260, CVE-2016-3264, CVE-2016-3265, CVE-2016-3269, CVE-2016-3271, CVE-2016-3273, CVE-2016-3274, CVE-2016-3276, CVE-2016-3277

[Update Details](#)

Recommendation is updated

20303 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution V (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3269

[Update Details](#)

Recommendation is updated

20304 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution IV (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3265

[Update Details](#)

Recommendation is updated

20305 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution III (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High
CVE: CVE-2016-3260

[Update Details](#)

Recommendation is updated

20306 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution II (3169999)

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

Risk Level: High
CVE: CVE-2016-3259

[Update Details](#)

Recommendation is updated

20307 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution I (3169999)

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

Risk Level: High
CVE: CVE-2016-3248

[Update Details](#)

Recommendation is updated

20325 - (MS16-085) Microsoft Edge Memory Corruption Remote Code Execution VI (3169999)

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

Risk Level: High
CVE: CVE-2016-3264

[Update Details](#)

Recommendation is updated

20374 - (MS16-096) Cumulative Security Update for Microsoft Edge (3177358)

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

Risk Level: High
CVE: CVE-2016-3289, CVE-2016-3293, CVE-2016-3296, CVE-2016-3319, CVE-2016-3322, CVE-2016-3326, CVE-2016-3327, CVE-2016-3329

[Update Details](#)

Recommendation is updated

20386 - (MS16-096) Microsoft Edge Browser Memory Corruption Remote Code Execution I (3177358)

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

Risk Level: High

CVE: CVE-2016-3289

[Update Details](#)

Recommendation is updated

20388 - (MS16-096) Microsoft Edge Chakra Javascript Engine Remote Code Execution (3177358)

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

Risk Level: High

CVE: CVE-2016-3296

[Update Details](#)

Recommendation is updated

20390 - (MS16-096) Microsoft Edge Browser Memory Corruption Remote Code Execution (3177358)

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

Risk Level: High

CVE: CVE-2016-3322

[Update Details](#)

Recommendation is updated

20482 - (MS16-110) Security Update for Microsoft Windows (3178467)

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

Risk Level: High

CVE: CVE-2016-3346, CVE-2016-3352, CVE-2016-3368, CVE-2016-3369

[Update Details](#)

Recommendation is updated

20505 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution II (3183043)

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

Risk Level: High

CVE: CVE-2016-3294

[Update Details](#)

Recommendation is updated

20506 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution III (3183043)

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

Risk Level: High

CVE: CVE-2016-3295

[Update Details](#)

Recommendation is updated

20509 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution VI (3183043)

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

Risk Level: High

CVE: CVE-2016-3350

[Update Details](#)

Recommendation is updated

20510 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution VII (3183043)

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

Risk Level: High

CVE: CVE-2016-3377

[Update Details](#)

Recommendation is updated

20624 - (MS16-119) Cumulative Security Update for Microsoft Edge (3192890)

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

Risk Level: High

CVE: CVE-2016-3267, CVE-2016-3331, CVE-2016-3382, CVE-2016-3386, CVE-2016-3387, CVE-2016-3388, CVE-2016-3389, CVE-2016-3390, CVE-2016-3391, CVE-2016-3392, CVE-2016-7189, CVE-2016-7190, CVE-2016-7194

[Update Details](#)

Recommendation is updated

20628 - (MS16-119) Microsoft Edge Browser Information Disclosure II (3192890)

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

Risk Level: High

CVE: CVE-2016-7189

[Update Details](#)

Recommendation is updated

20634 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution I (3192890)

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

Risk Level: High

CVE: CVE-2016-3386

[Update Details](#)

Recommendation is updated

20635 - (MS16-119) Microsoft Edge Browser Memory Corruption Remote Code Execution II (3192890)

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

Risk Level: High

CVE: CVE-2016-3382

[Update Details](#)

Recommendation is updated

20636 - (MS16-119) Microsoft Edge Browser Memory Corruption Remote Code Execution I (3192890)

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

Risk Level: High

CVE: CVE-2016-3331

[Update Details](#)

Recommendation is updated

20641 - (MS16-123) Microsoft Windows Win32k Privilege Escalation V (3192892)

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

Risk Level: High

CVE: CVE-2016-3376

[Update Details](#)

Recommendation is updated

20685 - (MS16-120) Microsoft Windows Graphics GDI+ Remote Code Execution (3192884)

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

Risk Level: High

CVE: CVE-2016-3396

[Update Details](#)

Recommendation is updated

20686 - (MS16-120) Microsoft Windows Graphics Component Remote Code Execution (3192884)

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

Risk Level: High

CVE: CVE-2016-3393

[Update Details](#)

Recommendation is updated

20687 - (MS16-122) Security Update for Microsoft Video Control (3195360)

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

Risk Level: High

CVE: CVE-2016-0142

Update Details

Recommendation is updated

20688 - (MS16-122) Microsoft Windows Video Control Remote Code Execution (3195360)

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

Risk Level: High

CVE: CVE-2016-0142

Update Details

Recommendation is updated

20754 - (MS16-130) Security Update for Microsoft Windows (3199172)

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

Risk Level: High

CVE: CVE-2016-7212, CVE-2016-7221, CVE-2016-7222

Update Details

Recommendation is updated

20759 - (MS16-135) Microsoft Windows Kernel Privilege Escalation IV (3199135)

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

Risk Level: High

CVE: CVE-2016-7255

Update Details

Recommendation is updated

20765 - (MS16-132) Security Update for Microsoft Graphics Component (3199120)

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

Risk Level: High

CVE: CVE-2016-7205, CVE-2016-7210, CVE-2016-7217

Update Details

Recommendation is updated

20767 - (MS16-132) Microsoft Windows Animation Manager Remote Code Execution (3199120)

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

Risk Level: High

CVE: CVE-2016-7205

Update Details

Recommendation is updated

20769 - (MS16-129) Microsoft Edge Browser Memory Corruption Remote Code Execution I (3199057)

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

Risk Level: High

CVE: CVE-2016-7196

Update Details

Recommendation is updated

20770 - (MS16-129) Microsoft Edge Browser Memory Corruption Remote Code Execution II (3199057)

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

Risk Level: High

CVE: CVE-2016-7198

Update Details

Recommendation is updated

20771 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution I (3199057)

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

Risk Level: High

CVE: CVE-2016-7200

Update Details

Recommendation is updated

20774 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution IV (3199057)

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

Risk Level: High

CVE: CVE-2016-7242

Update Details

Recommendation is updated

20783 - (MS16-129) Microsoft Edge Browser Memory Corruption Remote Code Execution VII (3199057)

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

Risk Level: High
CVE: CVE-2016-7240

[Update Details](#)

Recommendation is updated

20784 - (MS16-129) Microsoft Edge Browser Memory Corruption Remote Code Execution IV (3199057)

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

Risk Level: High
CVE: CVE-2016-7241

[Update Details](#)

Recommendation is updated

20785 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution VIII (3199057)

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

Risk Level: High
CVE: CVE-2016-7243

[Update Details](#)

Recommendation is updated

20795 - (MS16-134) Security Update for Common Log File System Driver (3193706)

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

Risk Level: High
CVE: CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, CVE-2016-7184

[Update Details](#)

Recommendation is updated

20828 - (MS16-130) Microsoft Windows File Manager Remote Code Execution (3199172)

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

Risk Level: High
CVE: CVE-2016-7212

[Update Details](#)

Recommendation is updated

20829 - (MS16-131) Microsoft Windows Video Control Remote Code Execution (3199151)

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

Risk Level: High

CVE: CVE-2016-7248

Update Details

Recommendation is updated

20958 - (MS16-146) Security Update for Microsoft Graphics Component (3204066)

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

Risk Level: High

CVE: CVE-2016-7257, CVE-2016-7272, CVE-2016-7273

Update Details

Recommendation is updated

20959 - (MS16-146) Microsoft Windows Graphics Remote Code Execution (3204066)

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

Risk Level: High

CVE: CVE-2016-7273

Update Details

Recommendation is updated

20960 - (MS16-146) Microsoft Windows Animation Manager Memory Corruption Remote Code Execution (3204066)

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

Risk Level: High

CVE: CVE-2016-7272

Update Details

Recommendation is updated

20971 - (MS16-147) Microsoft Windows Uniscribe Remote Code Execution (3204063)

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

Risk Level: High

CVE: CVE-2016-7274

Update Details

Recommendation is updated

20972 - (MS16-147) Security Update for Microsoft Uniscribe (3204063)

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

Risk Level: High

CVE: CVE-2016-7274

[Update Details](#)

Recommendation is updated

21437 - (MS17-009) Microsoft Windows PDF Library Remote Code Execution (4010319)

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

Risk Level: High

CVE: CVE-2017-0023

[Update Details](#)

Recommendation is updated

21438 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution II (4013076)

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

Risk Level: High

CVE: CVE-2017-0072

[Update Details](#)

Recommendation is updated

21439 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution III (4013076)

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

Risk Level: High

CVE: CVE-2017-0086

[Update Details](#)

Recommendation is updated

21440 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution IV (4013076)

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

Risk Level: High

CVE: CVE-2017-0087

[Update Details](#)

Recommendation is updated

21441 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution V (4013076)

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

Risk Level: High

CVE: CVE-2017-0088

[Update Details](#)

Recommendation is updated

21442 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution VI (4013076)

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

Risk Level: High

CVE: CVE-2017-0089

Update Details

Recommendation is updated

21443 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution VII (4013076)

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

Risk Level: High

CVE: CVE-2017-0090

Update Details

Recommendation is updated

21444 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution VIII (4013076)

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

Risk Level: High

CVE: CVE-2017-0083

Update Details

Recommendation is updated

21445 - (MS17-011) Microsoft Windows Uniscribe Remote Code Execution IX (4013076)

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

Risk Level: High

CVE: CVE-2017-0084

Update Details

Recommendation is updated

21482 - (MS17-009) Security Update for Microsoft Windows PDF Library (4010319)

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

Risk Level: High

CVE: CVE-2017-0023

Update Details

Recommendation is updated

21483 - (MS17-011) Security Update for Microsoft Uniscribe (4013076)

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

Risk Level: High

CVE: CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0085, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, CVE-2017-0090, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, CVE-2017-0128

Update Details

Recommendation is updated

32629 - Oracle Solaris 119060-71 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-3467, CVE-2007-1667, CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1986, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1992, CVE-2013-1993, CVE-2013-1995, CVE-2013-1996, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2063, CVE-2013-2064, CVE-2013-2066, CVE-2013-6462, CVE-2014-0209, CVE-2014-0210, CVE-2014-0211

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32633 - Oracle Solaris 119059-72 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-3467, CVE-2007-1667, CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1986, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1992, CVE-2013-1993, CVE-2013-1995, CVE-2013-1996, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2063, CVE-2013-2064, CVE-2013-2066, CVE-2013-6462, CVE-2014-0209, CVE-2014-0210, CVE-2014-0211

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

141082 - Red Hat Enterprise Linux RHSA-2016-0072 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8947, CVE-2016-1612, CVE-2016-1613, CVE-2016-1614, CVE-2016-1615, CVE-2016-1616, CVE-2016-1617, CVE-2016-1618, CVE-2016-1619, CVE-2016-1620, CVE-2016-2051, CVE-2016-2052

Update Details

CVE is updated

141089 - Red Hat Enterprise Linux RHSA-2016-0197 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1521, CVE-2016-1522, CVE-2016-1523, CVE-2016-1969

Update Details

CVE is updated FASLScript is updated

141124 - Red Hat Enterprise Linux RHSA-2016-0460 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1952, CVE-2016-1954, CVE-2016-1957, CVE-2016-1960, CVE-2016-1961, CVE-2016-1964, CVE-2016-1966, CVE-2016-1974, CVE-2016-1977, CVE-2016-2790, CVE-2016-2791, CVE-2016-2792, CVE-2016-2793, CVE-2016-2794, CVE-2016-2795, CVE-2016-2796, CVE-2016-2797, CVE-2016-2798, CVE-2016-2799, CVE-2016-2800, CVE-2016-2801, CVE-2016-2802

Update Details

FASLScript is updated

141134 - Red Hat Enterprise Linux RHSA-2016-0512 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0636

Update Details

FASLScript is updated

141139 - Red Hat Enterprise Linux RHSA-2016-0513 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0636

Update Details

FASLScript is updated

141147 - Red Hat Enterprise Linux RHSA-2016-0594 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1521, CVE-2016-1522, CVE-2016-1523, CVE-2016-1526

Update Details

FASLScript is updated

141195 - Red Hat Enterprise Linux RHSA-2016-1025 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2328, CVE-2015-3217, CVE-2015-5073, CVE-2015-8385, CVE-2015-8386, CVE-2015-8388, CVE-2015-8391, CVE-2016-3191

Update Details

FASLScript is updated

141204 - Red Hat Enterprise Linux RHSA-2016-1132 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3210, CVE-2015-3217, CVE-2015-4792, CVE-2015-4802, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4879, CVE-2015-4895, CVE-2015-4913, CVE-2015-5073, CVE-2015-8381, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8388, CVE-2015-8391, CVE-2015-8392, CVE-2015-8395, CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0610, CVE-2016-0616, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0651, CVE-2016-0655, CVE-2016-0666, CVE-2016-0668, CVE-2016-1283, CVE-2016-2047, CVE-2016-3191

[Update Details](#)

FASLScript is updated

141232 - Red Hat Enterprise Linux RHSA-2016-1458 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3458, CVE-2016-3500, CVE-2016-3508, CVE-2016-3550, CVE-2016-3587, CVE-2016-3598, CVE-2016-3606, CVE-2016-3610

[Update Details](#)

FASLScript is updated

141236 - Red Hat Enterprise Linux RHSA-2016-1504 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3458, CVE-2016-3500, CVE-2016-3508, CVE-2016-3550, CVE-2016-3598, CVE-2016-3606, CVE-2016-3610

[Update Details](#)

FASLScript is updated

141253 - Red Hat Enterprise Linux RHSA-2016-1588 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3511, CVE-2016-3598

[Update Details](#)

FASLScript is updated

141259 - Red Hat Enterprise Linux RHSA-2016-1587 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3511, CVE-2016-3598

[Update Details](#)

FASLScript is updated

141312 - Red Hat Enterprise Linux RHSA-2016-2136 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5573, CVE-2016-5597

[Update Details](#)

FASLScript is updated

141319 - Red Hat Enterprise Linux RHSA-2016-2137 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5573, CVE-2016-5597

[Update Details](#)

FASLScript is updated

141325 - Red Hat Enterprise Linux RHSA-2016-2580 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

[Update Details](#)

FASLScript is updated

141355 - Red Hat Enterprise Linux RHSA-2016-2579 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0794, CVE-2016-0795

[Update Details](#)

FASLScript is updated

141359 - Red Hat Enterprise Linux RHSA-2016-2658 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

[Update Details](#)

CVE is updated FASLScript is updated

141367 - Red Hat Enterprise Linux RHSA-2016-2780 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-9064, CVE-2016-9066

[Update Details](#)

FASLScript is updated

141368 - Red Hat Enterprise Linux RHSA-2016-2779 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2834, CVE-2016-5285, CVE-2016-8635

[Update Details](#)

FASLScript is updated

141376 - Red Hat Enterprise Linux RHSA-2016-2843 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

[Update Details](#)

FASLScript is updated

141384 - Red Hat Enterprise Linux RHSA-2016-2946 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

[Update Details](#)

FASLScript is updated

141392 - Red Hat Enterprise Linux RHSA-2017-0002 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1669, CVE-2016-5180, CVE-2016-5325, CVE-2016-7099

[Update Details](#)

FASLScript is updated

20755 - (MS16-131) Security Update for Microsoft Video Control (3199151)

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

Risk Level: High

CVE: CVE-2016-7248

[Update Details](#)

Recommendation is updated

21099 - (MS17-001) Cumulative Security Update for Microsoft Edge (3214288)

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

Risk Level: High

CVE: CVE-2017-0002

Update Details

Recommendation is updated

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

Update Details

FASLScript 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

20026 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution I (3155538)

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

Risk Level: High

CVE: CVE-2016-0186

Update Details

Recommendation is updated

20027 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution II (3155538)

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

Risk Level: High

CVE: CVE-2016-0191

Update Details

Recommendation is updated

20028 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution III (3155538)

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

Risk Level: High

CVE: CVE-2016-0193

Update Details

Recommendation is updated

20029 - (MS16-052) Microsoft Edge Memory Corruption Remote Code Execution (3155538)

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

Risk Level: High

CVE: CVE-2016-0192

Update Details

Recommendation is updated

20043 - (MS16-060) Microsoft Windows Kernel Symbolic Links Privilege Escalation (3154846)

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

Risk Level: High

CVE: CVE-2016-0180

Update Details

Recommendation is updated

20048 - (MS16-060) Security Update for Windows Kernel (3154846)

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

Risk Level: High

CVE: CVE-2016-0180

Update Details

Recommendation is updated

20064 - (MS16-052) Cumulative Security Update for Microsoft Edge (3155538)

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

Risk Level: High

CVE: CVE-2016-0186, CVE-2016-0191, CVE-2016-0192, CVE-2016-0193

Update Details

Recommendation is updated

20152 - (MS16-068) Microsoft Edge Chakra Scripting Engine Memory Corruption Remote Code Execution II (3163656)

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

Risk Level: High

CVE: CVE-2016-3202

Update Details

Recommendation is updated

20155 - (MS16-068) Microsoft Edge Memory Corruption Remote Code Execution (3163656)

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

Risk Level: High

CVE: CVE-2016-3222

Update Details

Recommendation is updated

20274 - (MS16-087) Microsoft Windows Print Spooler File System Writing Privilege Escalation (3170005)

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

Risk Level: High

CVE: CVE-2016-3239

Update Details

Recommendation is updated

20309 - (MS16-085) Microsoft Edge Memory Corruption Remote Code Execution I (3169999)

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

Risk Level: High

CVE: CVE-2016-3246

Update Details

Recommendation is updated

20389 - (MS16-096) Microsoft Edge PDF Remote Code Execution (3177358)

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

Risk Level: High

CVE: CVE-2016-3319

Update Details

Recommendation is updated

20503 - (MS16-105) Cumulative Security Update for Microsoft Edge (3183043)

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

Risk Level: High

CVE: CVE-2016-3247, CVE-2016-3291, CVE-2016-3294, CVE-2016-3295, CVE-2016-3297, CVE-2016-3325, CVE-2016-3330, CVE-2016-3350, CVE-2016-3351, CVE-2016-3370, CVE-2016-3374, CVE-2016-3377

Update Details

Recommendation is updated

20631 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution IV (3192890)

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

Risk Level: High

CVE: CVE-2016-7190

Update Details

Recommendation is updated

20632 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution III (3192890)

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

Risk Level: High

CVE: CVE-2016-3390

Update Details

Recommendation is updated

20633 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution II (3192890)

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

Risk Level: High

CVE: CVE-2016-3389

[Update Details](#)

Recommendation is updated

20642 - (MS16-123) Microsoft Windows Win32k Privilege Escalation IV (3192892)

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

Risk Level: High

CVE: CVE-2016-7211

[Update Details](#)

Recommendation is updated

20643 - (MS16-123) Microsoft Windows Win32k Privilege Escalation III (3192892)

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

Risk Level: High

CVE: CVE-2016-7185

[Update Details](#)

Recommendation is updated

20644 - (MS16-123) Microsoft Windows Win32k Privilege Escalation II (3192892)

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

Risk Level: High

CVE: CVE-2016-3241

[Update Details](#)

Recommendation is updated

20663 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution V (3192890)

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

Risk Level: High

CVE: CVE-2016-7194

[Update Details](#)

Recommendation is updated

20676 - (MS16-125) Microsoft Windows Diagnostics Hub Privilege Escalation (3193229)

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

Risk Level: High

CVE: CVE-2016-7188

[Update Details](#)

Recommendation is updated

20677 - (MS16-125) Security Update for Diagnostic Hub (3193229)

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

Risk Level: High

CVE: CVE-2016-7188

Update Details

Recommendation is updated

20757 - (MS16-135) Security Update for Windows Kernel-Mode Drivers (3199135)

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

Risk Level: High

CVE: CVE-2016-7214, CVE-2016-7215, CVE-2016-7218, CVE-2016-7246, CVE-2016-7255

Update Details

Recommendation is updated

20772 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution II (3199057)

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

Risk Level: High

CVE: CVE-2016-7201

Update Details

Recommendation is updated

20794 - (MS16-129) Cumulative Security Update for Microsoft Edge (3199057)

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

Risk Level: High

CVE: CVE-2016-7195, CVE-2016-7196, CVE-2016-7198, CVE-2016-7199, CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7204, CVE-2016-7208, CVE-2016-7209, CVE-2016-7227, CVE-2016-7239, CVE-2016-7240, CVE-2016-7241, CVE-2016-7242, CVE-2016-7243

Update Details

Recommendation is updated

20796 - (MS16-137) Security Update for Windows Authentication Methods (3199173)

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

Risk Level: High

CVE: CVE-2016-7220, CVE-2016-7237, CVE-2016-7238

Update Details

Recommendation is updated

20975 - (MS16-151) Security Update for Windows Kernel-Mode Drivers (3205651)

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

Risk Level: High

CVE: CVE-2016-7259, CVE-2016-7260

Update Details

Recommendation is updated

20978 - (MS16-149) Security Update for Microsoft Windows (3205655)

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

Risk Level: High

CVE: CVE-2016-7219, CVE-2016-7292

Update Details

Recommendation is updated

20979 - (MS16-145) Microsoft Edge Scripting Engine Remote Code Execution III (3204062)

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

Risk Level: High

CVE: CVE-2016-7297

Update Details

Recommendation is updated

20980 - (MS16-145) Microsoft Edge Scripting Engine Remote Code Execution IV (3204062)

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

Risk Level: High

CVE: CVE-2016-7296

Update Details

Recommendation is updated

20981 - (MS16-145) Microsoft Edge Memory Handling Remote Code Execution III (3204062)

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

Risk Level: High

CVE: CVE-2016-7288

Update Details

Recommendation is updated

20982 - (MS16-145) Microsoft Edge Scripting Engine Remote Code Execution I (3204062)

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

Risk Level: High

CVE: CVE-2016-7287

[Update Details](#)

Recommendation is updated

20987 - (MS16-145) Microsoft Edge Memory Handling Remote Code Execution (3204062)

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

Risk Level: High

CVE: CVE-2016-7279

[Update Details](#)

Recommendation is updated

20993 - (MS16-145) Cumulative Security Update for Microsoft Edge (3204062)

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

Risk Level: High

CVE: CVE-2016-7181, CVE-2016-7206, CVE-2016-7279, CVE-2016-7280, CVE-2016-7281, CVE-2016-7282, CVE-2016-7286, CVE-2016-7287, CVE-2016-7288, CVE-2016-7296, CVE-2016-7297

[Update Details](#)

Recommendation is updated

21345 - (MS17-007) Security Update for Microsoft Edge (4013071)

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

Risk Level: High

CVE: CVE-2017-0009, CVE-2017-0010, CVE-2017-0011, CVE-2017-0012, CVE-2017-0015, CVE-2017-0017, CVE-2017-0023, CVE-2017-0032, CVE-2017-0033, CVE-2017-0034, CVE-2017-0035, CVE-2017-0037, CVE-2017-0065, CVE-2017-0066, CVE-2017-0067, CVE-2017-0068, CVE-2017-0069, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0135, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0140, CVE-2017-0141, CVE-2017-0150, CVE-2017-0151

[Update Details](#)

Recommendation is updated

21346 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution X (4013071)

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

Risk Level: High

CVE: CVE-2017-0133

[Update Details](#)

Recommendation is updated

21347 - (MS17-007) Microsoft Edge Memory Corruption Remote Code Execution IV (4013071)

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

Risk Level: High

CVE: CVE-2017-0134

Update Details

Recommendation is updated

21349 - (MS17-007) Microsoft Edge Memory Corruption Remote Code Execution V (4013071)

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

Risk Level: High

CVE: CVE-2017-0136

Update Details

Recommendation is updated

21350 - (MS17-007) Microsoft Edge Memory Corruption Remote Code Execution VI (4013071)

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

Risk Level: High

CVE: CVE-2017-0137

Update Details

Recommendation is updated

21351 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution XI (4013071)

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

Risk Level: High

CVE: CVE-2017-0138

Update Details

Recommendation is updated

21353 - (MS17-007) Microsoft Edge Memory Corruption Remote Code Execution III (4013071)

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

Risk Level: High

CVE: CVE-2017-0132

Update Details

Recommendation is updated

21354 - (MS17-007) Microsoft Edge Memory Handling Remote Code Execution (4013071)

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

Risk Level: High

CVE: CVE-2017-0131

Update Details

Recommendation is updated

21355 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution IX (4013071)

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

Risk Level: High

CVE: CVE-2017-0094

Update Details

Recommendation is updated

21356 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution VII (4013071)

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

Risk Level: High

CVE: CVE-2017-0071

Update Details

Recommendation is updated

21357 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution VI (4013071)

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

Risk Level: High

CVE: CVE-2017-0070

Update Details

Recommendation is updated

21360 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution V (4013071)

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

Risk Level: High

CVE: CVE-2017-0067

Update Details

Recommendation is updated

21363 - (MS17-007) Microsoft Edge Browser Remote Code Execution (4013071)

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

Risk Level: High

CVE: CVE-2017-0037

Update Details

Recommendation is updated

21365 - (MS17-007) Microsoft Edge Memory Corruption Remote Code Execution II (4013071)

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

Risk Level: High

CVE: CVE-2017-0035

Update Details

Recommendation is updated

21366 - (MS17-007) Microsoft Edge Memory Corruption Remote Code Execution I (4013071)

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

Risk Level: High

CVE: CVE-2017-0034

Update Details

Recommendation is updated

21368 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution III (4013071)

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

Risk Level: High

CVE: CVE-2017-0032

Update Details

Recommendation is updated

21369 - (MS17-007) Microsoft Edge PDF Remote Code Execution (4010319)

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

Risk Level: High

CVE: CVE-2017-0023

Update Details

Recommendation is updated

21371 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution II (4013071)

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

Risk Level: High
CVE: CVE-2017-0015

[Update Details](#)

Recommendation is updated

21374 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution I (4013071)

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

Risk Level: High
CVE: CVE-2017-0010

[Update Details](#)

Recommendation is updated

21376 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution (4013071)

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

Risk Level: High
CVE: CVE-2017-0141

[Update Details](#)

Recommendation is updated

21486 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution XIII (4013071)

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

Risk Level: High
CVE: CVE-2017-0150

[Update Details](#)

Recommendation is updated

21487 - (MS17-007) Microsoft Edge Scripting Engine Remote Code Execution XIV (4013071)

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

Risk Level: High
CVE: CVE-2017-0151

[Update Details](#)

Recommendation is updated

32160 - Oracle Solaris 136882-06 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32163 - Oracle Solaris 136883-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33116 - Oracle Solaris 150383-18 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-0166, CVE-2013-0169, CVE-2014-0224, CVE-2014-3508, CVE-2014-3511, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33222 - Oracle Solaris 125720-68 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-1526, CVE-2006-3467, CVE-2006-3739, CVE-2006-3740, CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, CVE-2011-4028, CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1986, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1992, CVE-2013-1993, CVE-2013-1995, CVE-2013-1996, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2063, CVE-2013-2064, CVE-2013-2066, CVE-2013-4396, CVE-2014-0209, CVE-2014-0210, CVE-2014-0211, CVE-2014-0397

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

140657 - Red Hat Enterprise Linux RHSA-2015-0093 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7923, CVE-2014-7924, CVE-2014-7925, CVE-2014-7926, CVE-2014-7927, CVE-2014-7928, CVE-2014-7929, CVE-2014-7930, CVE-2014-7931, CVE-2014-7932, CVE-2014-7933, CVE-2014-7934, CVE-2014-7935, CVE-2014-7936, CVE-2014-7937, CVE-2014-7938, CVE-2014-7939, CVE-2014-7940, CVE-2014-7941, CVE-2014-7942, CVE-2014-7943, CVE-2014-7944, CVE-2014-7945, CVE-2014-7946, CVE-2014-7947, CVE-2014-7948, CVE-2015-1346

Update Details

CVE is updated

140705 - Red Hat Enterprise Linux RHSA-2015-0627 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1213, CVE-2015-1214, CVE-2015-1215, CVE-2015-1216, CVE-2015-1217, CVE-2015-1218, CVE-2015-1219, CVE-2015-1220, CVE-2015-1221, CVE-2015-1222, CVE-2015-1223, CVE-2015-1224, CVE-2015-1225, CVE-2015-1226, CVE-2015-1227, CVE-2015-1228, CVE-2015-1229, CVE-2015-1230, CVE-2015-1231, CVE-2015-1232

[Update Details](#)

CVE is updated

140772 - Red Hat Enterprise Linux RHSA-2015-0715 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2016-0703, CVE-2016-0704

[Update Details](#)

CVE is updated

140773 - Red Hat Enterprise Linux RHSA-2015-0716 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2016-0703, CVE-2016-0704

[Update Details](#)

CVE is updated

140788 - Red Hat Enterprise Linux RHSA-2015-0800 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8275, CVE-2015-0204, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2016-0703, CVE-2016-0704

[Update Details](#)

CVE is updated

140807 - Red Hat Enterprise Linux RHSA-2015-0988 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0797, CVE-2015-2708, CVE-2015-2710, CVE-2015-2713, CVE-2015-2716, CVE-2015-4496

[Update Details](#)

CVE is updated

140826 - Red Hat Enterprise Linux RHSA-2015-1066 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8142, CVE-2014-9427, CVE-2014-9652, CVE-2014-9705, CVE-2014-9709, CVE-2015-0231, CVE-2015-0232, CVE-2015-0273, CVE-2015-1351, CVE-2015-2301, CVE-2015-2305, CVE-2015-2348, CVE-2015-2783, CVE-2015-2787, CVE-2015-3307, CVE-2015-3329, CVE-2015-3330, CVE-2015-3411, CVE-2015-3412, CVE-2015-4147, CVE-2015-4148, CVE-2015-4599, CVE-2015-4600, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE-2015-8935

[Update Details](#)

CVE is updated

140843 - Red Hat Enterprise Linux RHSA-2015-1135 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-7243, CVE-2014-8142, CVE-2014-9652, CVE-2014-9705, CVE-2014-9709, CVE-2015-0231, CVE-2015-0232, CVE-2015-0273, CVE-2015-2301, CVE-2015-2348, CVE-2015-2783, CVE-2015-2787, CVE-2015-3307, CVE-2015-3329, CVE-2015-3330, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4147, CVE-2015-4148, CVE-2015-4598, CVE-2015-4599, CVE-2015-4600, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE-2015-4643

[Update Details](#)

CVE is updated

140848 - Red Hat Enterprise Linux RHSA-2015-1187 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-7243, CVE-2015-2783, CVE-2015-3307, CVE-2015-3329, CVE-2015-3330, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4598, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE-2015-4643, CVE-2015-4644

[Update Details](#)

CVE is updated FASLScript is updated

140854 - Red Hat Enterprise Linux RHSA-2015-1186 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-7243, CVE-2015-2783, CVE-2015-3307, CVE-2015-3329, CVE-2015-3330, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4598, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE-2015-4643, CVE-2015-4644

[Update Details](#)

CVE is updated FASLScript is updated

140858 - Red Hat Enterprise Linux RHSA-2015-1219 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-7243, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4598, CVE-2015-4643, CVE-2015-4644

[Update Details](#)

FASLScript is updated

140891 - Red Hat Enterprise Linux RHSA-2015-1499 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1270, CVE-2015-1271, CVE-2015-1272, CVE-2015-1273, CVE-2015-1274, CVE-2015-1276, CVE-2015-1277, CVE-2015-1278, CVE-2015-1279, CVE-2015-1280, CVE-2015-1281, CVE-2015-1282, CVE-2015-1283, CVE-2015-1284, CVE-2015-1285, CVE-2015-1286, CVE-2015-1287, CVE-2015-1288, CVE-2015-1289, CVE-2015-5605

Update Details

CVE is updated

140910 - Red Hat Enterprise Linux RHSA-2015-1628 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6568, CVE-2015-0374, CVE-2015-0381, CVE-2015-0382, CVE-2015-0391, CVE-2015-0411, CVE-2015-0432, CVE-2015-0433, CVE-2015-0441, CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2582, CVE-2015-2620, CVE-2015-2643, CVE-2015-2648, CVE-2015-4737, CVE-2015-4752, CVE-2015-4757, CVE-2015-4816, CVE-2015-4819, CVE-2015-4864, CVE-2015-4879

Update Details

CVE is updated

140948 - Red Hat Enterprise Linux RHSA-2015-1841 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1302, CVE-2015-1303, CVE-2015-1304

Update Details

CVE is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

141021 - Red Hat Enterprise Linux RHSA-2015-2519 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7189, CVE-2015-7193, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

[Update Details](#)

FASLScript is updated

141022 - Red Hat Enterprise Linux RHSA-2015-2523 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

[Update Details](#)

FASLScript is updated

141026 - Red Hat Enterprise Linux RHSA-2015-2515 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7545

[Update Details](#)

Risk is updated CVE is updated FASLScript is updated

141027 - Red Hat Enterprise Linux RHSA-2015-2561 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7545

[Update Details](#)

FASLScript is updated

141032 - Red Hat Enterprise Linux RHSA-2015-2596 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

[Update Details](#)

FASLScript is updated

141041 - Red Hat Enterprise Linux RHSA-2015-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

[Update Details](#)

FASLScript is updated

141072 - Red Hat Enterprise Linux RHSA-2016-0064 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0728

[Update Details](#)

FASLScript is updated

141078 - Red Hat Enterprise Linux RHSA-2016-0099 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5041, CVE-2015-7575, CVE-2015-7981, CVE-2015-8126, CVE-2015-8472, CVE-2015-8540, CVE-2016-0402, CVE-2016-0448, CVE-2016-0466, CVE-2016-0483, CVE-2016-0494

[Update Details](#)

FASLScript is updated

141079 - Red Hat Enterprise Linux RHSA-2016-0098 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5041, CVE-2015-7575, CVE-2015-8126, CVE-2015-8472, CVE-2016-0402, CVE-2016-0448, CVE-2016-0466, CVE-2016-0475, CVE-2016-0483, CVE-2016-0494

[Update Details](#)

FASLScript is updated

141085 - Red Hat Enterprise Linux RHSA-2016-0204 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0741

[Update Details](#)

FASLScript is updated

141087 - Red Hat Enterprise Linux RHSA-2016-0185 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5157, CVE-2015-7872

[Update Details](#)

FASLScript is updated

141109 - Red Hat Enterprise Linux RHSA-2016-0430 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0729

[Update Details](#)

FASLScript is updated

141119 - Red Hat Enterprise Linux RHSA-2016-0457 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5589, CVE-2015-5590, CVE-2015-6831, CVE-2015-6832, CVE-2015-6833, CVE-2015-6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838, CVE-2015-7803, CVE-2015-7804

[Update Details](#)

FASLScript is updated

141146 - Red Hat Enterprise Linux RHSA-2016-0534 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4879, CVE-2015-4913, CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0616, CVE-2016-0642, CVE-2016-0651, CVE-2016-2047, CVE-2016-3471

[Update Details](#)

CVE is updated FASLScript is updated

141182 - Red Hat Enterprise Linux RHSA-2016-0724 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3710

[Update Details](#)

FASLScript is updated

141193 - Red Hat Enterprise Linux RHSA-2016-1033 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0758, CVE-2016-3044

[Update Details](#)

CVE is updated FASLScript is updated

141215 - Red Hat Enterprise Linux RHSA-2016-1293 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4444, CVE-2016-4446, CVE-2016-4989

Update Details

FASLScript is updated

141217 - Red Hat Enterprise Linux RHSA-2016-1277 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8767, CVE-2016-4565

Update Details

FASLScript is updated

141223 - Red Hat Enterprise Linux RHSA-2016-1425 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0742, CVE-2016-0746, CVE-2016-0747, CVE-2016-4450

Update Details

FASLScript is updated

141227 - Red Hat Enterprise Linux RHSA-2016-1480 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4815, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4913, CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0616, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0651, CVE-2016-0666, CVE-2016-2047, CVE-2016-3452, CVE-2016-3471, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5444

Update Details

FASLScript is updated

141228 - Red Hat Enterprise Linux RHSA-2016-1481 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4879, CVE-2015-4913, CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0616, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0651, CVE-2016-0666, CVE-2016-2047, CVE-2016-3452, CVE-2016-3471, CVE-2016-5444

[Update Details](#)

FASLScript is updated

141238 - Red Hat Enterprise Linux RHSA-2016-1546 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8127, CVE-2014-8129, CVE-2014-8130, CVE-2014-9330, CVE-2014-9655, CVE-2015-1547, CVE-2015-7554, CVE-2015-8665, CVE-2015-8668, CVE-2015-8683, CVE-2015-8781, CVE-2015-8782, CVE-2015-8783, CVE-2015-8784, CVE-2016-3632, CVE-2016-3945, CVE-2016-3990, CVE-2016-3991, CVE-2016-5320

[Update Details](#)

FASLScript is updated

141239 - Red Hat Enterprise Linux RHSA-2016-1539 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8660, CVE-2016-2143, CVE-2016-4470

[Update Details](#)

FASLScript is updated

141241 - Red Hat Enterprise Linux RHSA-2016-1551 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2830, CVE-2016-2836, CVE-2016-2837, CVE-2016-2838, CVE-2016-5252, CVE-2016-5254, CVE-2016-5258, CVE-2016-5259, CVE-2016-5262, CVE-2016-5263, CVE-2016-5264, CVE-2016-5265

[Update Details](#)

FASLScript is updated

141248 - Red Hat Enterprise Linux RHSA-2016-1604 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440

[Update Details](#)

FASLScript is updated

141249 - Red Hat Enterprise Linux RHSA-2016-1617 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565

[Update Details](#)

FASLScript is updated

141251 - Red Hat Enterprise Linux RHSA-2016-1602 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0640, CVE-2016-0641, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-3452, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5444

Update Details

FASLScript is updated

141252 - Red Hat Enterprise Linux RHSA-2016-1603 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440

Update Details

FASLScript is updated

141256 - Red Hat Enterprise Linux RHSA-2016-1601 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3459, CVE-2016-3477, CVE-2016-3486, CVE-2016-3501, CVE-2016-3521, CVE-2016-3614, CVE-2016-3615, CVE-2016-5439, CVE-2016-5440, CVE-2016-5609, CVE-2016-5612, CVE-2016-5627, CVE-2016-5630, CVE-2016-8284, CVE-2016-8288

Update Details

CVE is updated FASLScript is updated

141262 - Red Hat Enterprise Linux RHSA-2016-1637 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440

Update Details

FASLScript is updated

141284 - Red Hat Enterprise Linux RHSA-2016-1847 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-6197, CVE-2016-6198

Update Details

CVE is updated FASLScript is updated

141286 - Red Hat Enterprise Linux RHSA-2016-1912 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5250, CVE-2016-5257, CVE-2016-5261, CVE-2016-5270, CVE-2016-5272, CVE-2016-5274, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5280, CVE-2016-5281, CVE-2016-5284

[Update Details](#)

FASLScript is updated

141287 - Red Hat Enterprise Linux RHSA-2016-1940 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6304, CVE-2016-6306

[Update Details](#)

FASLScript is updated

141288 - Red Hat Enterprise Linux RHSA-2016-1944 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

[Update Details](#)

FASLScript is updated

141289 - Red Hat Enterprise Linux RHSA-2016-1978 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000111

[Update Details](#)

FASLScript is updated

141295 - Red Hat Enterprise Linux RHSA-2016-1985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5257

[Update Details](#)

FASLScript is updated

141298 - Red Hat Enterprise Linux RHSA-2016-2047 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7039

[Update Details](#)

FASLScript is updated

141308 - Red Hat Enterprise Linux RHSA-2016-2098 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Update Details

FASLScript is updated

141310 - Red Hat Enterprise Linux RHSA-2016-2099 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776, CVE-2016-2848

Update Details

FASLScript is updated

141318 - Red Hat Enterprise Linux RHSA-2016-2132 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Update Details

FASLScript is updated

141323 - Red Hat Enterprise Linux RHSA-2016-2582 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8803, CVE-2015-8804, CVE-2015-8805, CVE-2016-6489

Update Details

FASLScript is updated

141337 - Red Hat Enterprise Linux RHSA-2016-2588 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

Update Details

FASLScript is updated

141338 - Red Hat Enterprise Linux RHSA-2016-2598 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5399, CVE-2016-5766, CVE-2016-5767, CVE-2016-5768

[Update Details](#)

FASLScript is updated

141342 - Red Hat Enterprise Linux RHSA-2016-2590 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2774

[Update Details](#)

FASLScript is updated

141351 - Red Hat Enterprise Linux RHSA-2016-2573 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5229, CVE-2015-5277, CVE-2016-3075

[Update Details](#)

FASLScript is updated

141365 - Red Hat Enterprise Linux RHSA-2016-2702 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7545

[Update Details](#)

FASLScript is updated

141369 - Red Hat Enterprise Linux RHSA-2016-2802 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6304

[Update Details](#)

FASLScript is updated

141371 - Red Hat Enterprise Linux RHSA-2016-2825 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5290

[Update Details](#)

FASLScript is updated

141373 - Red Hat Enterprise Linux RHSA-2016-2824 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2016-0718

[Update Details](#)

FASLScript is updated

141374 - Red Hat Enterprise Linux RHSA-2016-2819 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

[Update Details](#)

FASLScript is updated

141375 - Red Hat Enterprise Linux RHSA-2016-2850 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

[Update Details](#)

FASLScript is updated

141386 - Red Hat Enterprise Linux RHSA-2016-2973 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9905

[Update Details](#)

FASLScript 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

20184 - (MS16-078) Security Update for Windows Diagnostic Hub (3165479)

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

Risk Level: Medium

CVE: CVE-2016-3231

Update Details

Recommendation is updated

20626 - (MS16-119) Microsoft Edge Browser Privilege Escalation II (3192890)

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

Risk Level: Medium

CVE: CVE-2016-3387

Update Details

Recommendation is updated

20756 - (MS16-140) Security Update for Boot Manager (3193479)

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

Risk Level: Medium

CVE: CVE-2016-7247

Update Details

Recommendation is updated

20957 - (MS16-150) Security Update for Windows Secure Kernel Mode (3205642)

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

Risk Level: Medium

CVE: CVE-2016-7271

Update Details

Recommendation is updated

21025 - (SB10181) McAfee VirusScan Enterprise Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-8016, CVE-2016-8017, CVE-2016-8018, CVE-2016-8019, CVE-2016-8020, CVE-2016-8021, CVE-2016-8022, CVE-2016-8023, CVE-2016-8024, CVE-2016-8025

Update Details

Risk is updated

31558 - Oracle Solaris 119783-40 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-1447, CVE-2009-0696, CVE-2010-3613, CVE-2010-3614, CVE-2011-1910, CVE-2011-2464, CVE-2011-4313, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2013-0415, CVE-2014-0591

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

31564 - Oracle Solaris 119784-40 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-1447, CVE-2009-0696, CVE-2010-3613, CVE-2010-3614, CVE-2011-1910, CVE-2011-2464, CVE-2011-4313, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2013-0415, CVE-2014-0591

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

140912 - Red Hat Enterprise Linux RHSA-2015-1630 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2582, CVE-2015-2611, CVE-2015-2617, CVE-2015-2620, CVE-2015-2639, CVE-2015-2641, CVE-2015-2643, CVE-2015-2648, CVE-2015-2661, CVE-2015-4737, CVE-2015-4752, CVE-2015-4756, CVE-2015-4757, CVE-2015-4761, CVE-2015-4766, CVE-2015-4767, CVE-2015-4769, CVE-2015-4771, CVE-2015-4772, CVE-2015-4819, CVE-2015-4833, CVE-2015-4864, CVE-2015-4879, CVE-2015-4895, CVE-2015-4904

Update Details

CVE is updated FASLScript is updated

140928 - Red Hat Enterprise Linux RHSA-2015-1646 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2571, CVE-2015-2582, CVE-2015-2611, CVE-2015-2617, CVE-2015-2620, CVE-2015-2639, CVE-2015-2641, CVE-2015-2643, CVE-2015-2648, CVE-2015-2661, CVE-2015-3152, CVE-2015-4737, CVE-2015-4752, CVE-2015-4756, CVE-2015-4757, CVE-2015-4761, CVE-2015-4767, CVE-2015-4769, CVE-2015-4771, CVE-2015-4772, CVE-2015-4864, CVE-2015-4866

Update Details

CVE is updated FASLScript is updated

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-2015-3288, CVE-2015-3339, CVE-2015-4170, CVE-2015-5283, CVE-2015-6526, CVE-2015-7613, CVE-2015-7837, CVE-2015-8215, CVE-2016-0774

Update Details

CVE is updated FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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-2014-9750, CVE-2014-9751, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

141030 - Red Hat Enterprise Linux RHSA-2015-2550 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317, CVE-2015-8710

[Update Details](#)

FASLScript is updated

141036 - Red Hat Enterprise Linux RHSA-2015-2619 Update Is Not Installed

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

Risk Level: Medium

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

[Update Details](#)

FASLScript is updated

141039 - Red Hat Enterprise Linux RHSA-2015-2623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

[Update Details](#)

FASLScript is updated

141080 - Red Hat Enterprise Linux RHSA-2016-0073 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8704

Update Details

FASLScript is updated

141081 - Red Hat Enterprise Linux RHSA-2016-0083 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1714

Update Details

FASLScript is updated

141088 - Red Hat Enterprise Linux RHSA-2016-0176 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5229, CVE-2015-7547

Update Details

FASLScript is updated

141093 - Red Hat Enterprise Linux RHSA-2016-0225 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7547

Update Details

FASLScript is updated

141122 - Red Hat Enterprise Linux RHSA-2016-0370 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1950

Update Details

FASLScript is updated

141138 - Red Hat Enterprise Linux RHSA-2016-0495 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1950

[Update Details](#)

FASLScript is updated

141142 - Red Hat Enterprise Linux RHSA-2016-0532 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8629, CVE-2015-8630, CVE-2015-8631

[Update Details](#)

FASLScript is updated

141165 - Red Hat Enterprise Linux RHSA-2016-0685 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

[Update Details](#)

FASLScript is updated

141171 - Red Hat Enterprise Linux RHSA-2016-0706 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3068, CVE-2016-3069

[Update Details](#)

FASLScript is updated

141188 - Red Hat Enterprise Linux RHSA-2016-0855 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5313, CVE-2013-4312, CVE-2014-7842, CVE-2014-8134, CVE-2015-5156, CVE-2015-7509, CVE-2015-8215, CVE-2015-8324, CVE-2015-8543, CVE-2016-3841

[Update Details](#)

CVE is updated

141194 - Red Hat Enterprise Linux RHSA-2016-1086 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3698

[Update Details](#)

FASLScript is updated

141199 - Red Hat Enterprise Linux RHSA-2016-1141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

[Update Details](#)

FASLScript is updated

141202 - Red Hat Enterprise Linux RHSA-2016-1139 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-0801, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

[Update Details](#)

FASLScript is updated

141209 - Red Hat Enterprise Linux RHSA-2016-1217 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2828, CVE-2016-2831

[Update Details](#)

FASLScript is updated

141216 - Red Hat Enterprise Linux RHSA-2016-1296 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

[Update Details](#)

FASLScript is updated

141219 - Red Hat Enterprise Linux RHSA-2016-1392 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2818

[Update Details](#)

FASLScript is updated

141234 - Red Hat Enterprise Linux RHSA-2016-1486 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2119

[Update Details](#)

FASLScript is updated

141270 - Red Hat Enterprise Linux RHSA-2016-1781 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

Update Details

FASLScript is updated

141272 - Red Hat Enterprise Linux RHSA-2016-1809 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2836

Update Details

FASLScript is updated

141274 - Red Hat Enterprise Linux RHSA-2016-1820 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

Update Details

FASLScript is updated

141275 - Red Hat Enterprise Linux RHSA-2016-1821 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

Update Details

FASLScript is updated

141277 - Red Hat Enterprise Linux RHSA-2016-1844 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8916, CVE-2015-8917, CVE-2015-8919, CVE-2015-8920, CVE-2015-8921, CVE-2015-8922, CVE-2015-8923, CVE-2015-8924, CVE-2015-8925, CVE-2015-8926, CVE-2015-8928, CVE-2015-8930, CVE-2015-8931, CVE-2015-8932, CVE-2015-8934, CVE-2016-1541, CVE-2016-4300, CVE-2016-4302, CVE-2016-4809, CVE-2016-5418, CVE-2016-5844, CVE-2016-6250, CVE-2016-7166

Update Details

FASLScript is updated

141335 - Red Hat Enterprise Linux RHSA-2016-2606 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

Update Details

FASLScript is updated

141357 - Red Hat Enterprise Linux RHSA-2016-2589 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4994

Update Details

FASLScript is updated

141388 - Red Hat Enterprise Linux RHSA-2016-2972 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Update Details

FASLScript 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

19355 - (MS15-124) Microsoft Internet Explorer Script Engine Information Disclosure (3116180)

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

Risk Level: Medium

CVE: CVE-2015-6135

Update Details

Recommendation is updated

19385 - (MS15-124) Microsoft Internet Explorer XSS Filter Policies Enforcement Security Bypass (3116180)

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

Risk Level: Medium

CVE: CVE-2015-6164

[Update Details](#)

Recommendation is updated

19524 - (MS16-001) Microsoft Internet Explorer Cross Domain Privilege Escalation (3124903)

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

Risk Level: Medium

CVE: CVE-2016-0005

[Update Details](#)

Recommendation is updated

20141 - (MS16-077) Microsoft Windows WPAD Proxy Discovery Privilege Escalation (3165191)

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

Risk Level: Medium

CVE: CVE-2016-3236

[Update Details](#)

Recommendation is updated

20142 - (MS16-077) Microsoft Windows WPAD Privilege Escalation (3165191)

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

Risk Level: Medium

CVE: CVE-2016-3213

[Update Details](#)

Recommendation is updated

20149 - (MS16-068) Microsoft Edge Content Security Policy Security Bypass (3163656)

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

Risk Level: Medium

CVE: CVE-2016-3198

[Update Details](#)

Recommendation is updated

20151 - (MS16-068) Microsoft Edge PDF Information Disclosure (3163656)

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

Risk Level: Medium

CVE: CVE-2016-3201

[Update Details](#)

Recommendation is updated

20156 - (MS16-068) Microsoft Edge PDF Information Disclosure II (3163656)

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

Risk Level: Medium

CVE: CVE-2016-3215

[Update Details](#)

Recommendation is updated

20174 - (MS16-072) Microsoft Windows Group Policy Privilege Escalation (3163622)

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

Risk Level: Medium

CVE: CVE-2016-3223

[Update Details](#)

Recommendation is updated

20181 - (MS16-082) Windows Search Component Denial of Service Vulnerability (3165270)

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

Risk Level: Medium

CVE: CVE-2016-3230

[Update Details](#)

Recommendation is updated

20182 - (MS16-072) Security Update for Group Policy (3163622)

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

Risk Level: Medium

CVE: CVE-2016-3223

[Update Details](#)

Recommendation is updated

20183 - (MS16-078) Microsoft Windows Diagnostics Hub Privilege Escalation (3165479)

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

Risk Level: Medium

CVE: CVE-2016-3231

[Update Details](#)

Recommendation is updated

20185 - (MS16-082) Security Update for Microsoft Windows Search Component (3165270)

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

Risk Level: Medium

CVE: CVE-2016-3230

Update Details

Recommendation is updated

20280 - (MS16-091) Microsoft .NET Framework XML Parsing Information Disclosure (3170048)

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

Risk Level: Medium

CVE: CVE-2016-3255

Update Details

Recommendation is updated

20296 - (MS16-091) Security Update for .NET Framework (3170048)

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

Risk Level: Medium

CVE: CVE-2016-3255

Update Details

Recommendation is updated

20387 - (MS16-096) Microsoft Edge Browser Memory Corruption Remote Code Execution II (3177358)

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

Risk Level: Medium

CVE: CVE-2016-3293

Update Details

Recommendation is updated

20391 - (MS16-096) Microsoft Edge Browser Information Disclosure I (3177358)

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

Risk Level: Medium

CVE: CVE-2016-3326

Update Details

Recommendation is updated

20392 - (MS16-096) Microsoft Edge Browser Information Disclosure II (3177358)

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

Risk Level: Medium

CVE: CVE-2016-3327

Update Details

Recommendation is updated

20393 - (MS16-096) Microsoft Edge Browser Information Disclosure III (3177358)

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

Risk Level: Medium

CVE: CVE-2016-3329

Update Details

Recommendation is updated

20394 - (MS16-103) Microsoft Windows ActiveSyncProvider Information Disclosure (3182332)

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

Risk Level: Medium

CVE: CVE-2016-3312

Update Details

Recommendation is updated

20483 - (MS16-110) Microsoft Windows Memory Corruption Denial of Service (3178467)

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

Risk Level: Medium

CVE: CVE-2016-3369

Update Details

Recommendation is updated

20484 - (MS16-110) Microsoft Windows Memory Corruption Remote Code Execution (3178467)

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

Risk Level: Medium

CVE: CVE-2016-3368

Update Details

Recommendation is updated

20485 - (MS16-110) Microsoft Windows MSA Login Sessions NTLM Single Sign On Validation Information Disclosure (3178467)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3352

[Update Details](#)

Recommendation is updated

20486 - (MS16-110) Microsoft Windows Permissions Enforcement DLL Loading Privilege Escalation (3178467)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3346

[Update Details](#)

Recommendation is updated

20504 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution I (3183043)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3247

[Update Details](#)

Recommendation is updated

20507 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution IV (3183043)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3297

[Update Details](#)

Recommendation is updated

20508 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution V (3183043)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3330

[Update Details](#)

Recommendation is updated

20511 - (MS16-105) Microsoft Edge Browser Information Disclosure I (3183043)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3291

[Update Details](#)

Recommendation is updated

20512 - (MS16-105) Microsoft Edge Browser Information Disclosure II (3183043)

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

Risk Level: Medium

CVE: CVE-2016-3325

[Update Details](#)

Recommendation is updated

20513 - (MS16-105) Microsoft Edge Browser Information Disclosure III (3183043)

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

Risk Level: Medium

CVE: CVE-2016-3351

[Update Details](#)

Recommendation is updated

20514 - (MS16-105) Microsoft Edge Browser Information Disclosure IV (3183043)

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

Risk Level: Medium

CVE: CVE-2016-3374

[Update Details](#)

Recommendation is updated

20515 - (MS16-105) Microsoft Edge Browser Information Disclosure V (3183043)

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

Risk Level: Medium

CVE: CVE-2016-3370

[Update Details](#)

Recommendation is updated

20516 - (MS16-112) Security Update for Windows Lock Screen (3178469)

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

Risk Level: Medium

CVE: CVE-2016-3302

[Update Details](#)

Recommendation is updated

20517 - (MS16-112) Microsoft Windows Lock Screen Content Loading Privilege Escalation (3178469)

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

Risk Level: Medium

CVE: CVE-2016-3302

[Update Details](#)

Recommendation is updated

20518 - (MS16-113) Security Update for Windows Secure Kernel Mode (3185876)

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

Risk Level: Medium

CVE: CVE-2016-3344

[Update Details](#)

Recommendation is updated

20519 - (MS16-113) Microsoft Windows Secure Kernel Information Disclosure (3185876)

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

Risk Level: Medium

CVE: CVE-2016-3344

[Update Details](#)

Recommendation is updated

20682 - (MS16-120) Microsoft Windows Graphics GDI+ Information Disclosure III (3192884)

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

Risk Level: Medium

CVE: CVE-2016-3263

[Update Details](#)

Recommendation is updated

20683 - (MS16-120) Microsoft Windows Graphics GDI+ Information Disclosure II (3192884)

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

Risk Level: Medium

CVE: CVE-2016-3262

[Update Details](#)

Recommendation is updated

20684 - (MS16-120) Microsoft Windows Graphics GDI+ Information Disclosure I (3192884)

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

Risk Level: Medium

CVE: CVE-2016-3209

[Update Details](#)

Recommendation is updated

20760 - (MS16-135) Microsoft Windows Kernel Privilege Escalation I (3199135)

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

Risk Level: Medium

CVE: CVE-2016-7246

[Update Details](#)

Recommendation is updated

20761 - (MS16-135) Microsoft Windows Kernel Bowser.sys Information Disclosure (3199135)

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

Risk Level: Medium

CVE: CVE-2016-7218

[Update Details](#)

Recommendation is updated

20762 - (MS16-135) Microsoft Windows Kernel Privilege Escalation III (3199135)

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

Risk Level: Medium

CVE: CVE-2016-7215

[Update Details](#)

Recommendation is updated

20764 - (MS16-135) Microsoft Windows Kernel Information Disclosure II (3199135)

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

Risk Level: Medium

CVE: CVE-2016-7214

[Update Details](#)

Recommendation is updated

20766 - (MS16-132) Microsoft Windows Open Type Font Information Disclosure (3199120)

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

Risk Level: Medium

CVE: CVE-2016-7210

Update Details

Recommendation is updated

20768 - (MS16-132) Microsoft Windows Media Foundation Memory Corruption Vulnerability (3199120)

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

Risk Level: Medium

CVE: CVE-2016-7217

Update Details

Recommendation is updated

20773 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution III (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7203

Update Details

Recommendation is updated

20775 - (MS16-129) Microsoft Edge Browser Memory Corruption Remote Code Execution III (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7195

Update Details

Recommendation is updated

20776 - (MS16-129) Microsoft Edge Browser Information Disclosure (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7199

Update Details

Recommendation is updated

20777 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution V (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7202

Update Details

Recommendation is updated

20778 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Information Disclosure II (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7204

Update Details

Recommendation is updated

20779 - (MS16-129) Microsoft Edge HTTP Parsing Spoofing Remote Code Execution VI (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7208

Update Details

Recommendation is updated

20780 - (MS16-129) Microsoft Edge Browser Information Disclosure II (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7209

Update Details

Recommendation is updated

20781 - (MS16-129) Microsoft Edge Browser Cross Site Scripting Information Disclosure (3199057)

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

Risk Level: Medium

CVE: CVE-2016-7227

Update Details

Recommendation is updated

20782 - (MS16-129) Microsoft Edge Scripting Engine Memory Corruption Information Disclosure (3199057)

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

Risk Level: Medium
CVE: CVE-2016-7239

[Update Details](#)

Recommendation is updated

20786 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation I (3193706)

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

Risk Level: Medium
CVE: CVE-2016-0026

[Update Details](#)

Recommendation is updated

20787 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation II (3193706)

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

Risk Level: Medium
CVE: CVE-2016-3332

[Update Details](#)

Recommendation is updated

20788 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation III (3193706)

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

Risk Level: Medium
CVE: CVE-2016-3333

[Update Details](#)

Recommendation is updated

20789 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation IV (3193706)

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

Risk Level: Medium
CVE: CVE-2016-3334

[Update Details](#)

Recommendation is updated

20790 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation V (3193706)

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

Risk Level: Medium
CVE: CVE-2016-3335

[Update Details](#)

Recommendation is updated

20791 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation VI (3193706)

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

Risk Level: Medium

CVE: CVE-2016-3338

[Update Details](#)

Recommendation is updated

20792 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation VII (3193706)

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

Risk Level: Medium

CVE: CVE-2016-3340

[Update Details](#)

Recommendation is updated

20793 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation VIII (3193706)

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

Risk Level: Medium

CVE: CVE-2016-3342

[Update Details](#)

Recommendation is updated

20800 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation IX (3193706)

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

Risk Level: Medium

CVE: CVE-2016-3343

[Update Details](#)

Recommendation is updated

20801 - (MS16-134) Microsoft Windows Common Log File System Privilege Escalation X (3193706)

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

Risk Level: Medium

CVE: CVE-2016-7184

[Update Details](#)

Recommendation is updated

20802 - (MS16-137) Microsoft Windows Virtual Secure Mode Information Disclosure (3199173)

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

Risk Level: Medium

CVE: CVE-2016-7220

[Update Details](#)

Recommendation is updated

20803 - (MS16-137) Microsoft Windows Local Security Authority Denial of Service (3199173)

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

Risk Level: Medium

CVE: CVE-2016-7237

[Update Details](#)

Recommendation is updated

20805 - (MS16-137) Microsoft Windows Virtual Hard Drive Privilege Escalation (3199173)

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

Risk Level: Medium

CVE: CVE-2016-7238

[Update Details](#)

Recommendation is updated

20826 - (MS16-130) Microsoft Windows Task Scheduler Privilege Escalation (3199172)

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

Risk Level: Medium

CVE: CVE-2016-7222

[Update Details](#)

Recommendation is updated

20827 - (MS16-130) Microsoft Windows IME Privilege Escalation (3199172)

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

Risk Level: Medium

CVE: CVE-2016-7221

[Update Details](#)

Recommendation is updated

20836 - (MS16-138) Microsoft Windows Virtual Hard Drive Privilege Escalation IV (3199647)

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

Risk Level: Medium

CVE: CVE-2016-7226

Update Details

Recommendation is updated

20837 - (MS16-138) Microsoft Windows Virtual Hard Drive Privilege Escalation III (3199647)

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

Risk Level: Medium

CVE: CVE-2016-7225

Update Details

Recommendation is updated

20838 - (MS16-138) Microsoft Windows Virtual Hard Drive Privilege Escalation II (3199647)

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

Risk Level: Medium

CVE: CVE-2016-7224

Update Details

Recommendation is updated

20839 - (MS16-138) Microsoft Windows Virtual Hard Drive Privilege Escalation I (3199647)

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

Risk Level: Medium

CVE: CVE-2016-7223

Update Details

Recommendation is updated

20840 - (MS16-140) Microsoft Windows Secure Boot Security Bypass (3193479)

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

Risk Level: Medium

CVE: CVE-2016-7247

Update Details

Recommendation is updated

20857 - (MS16-132) Microsoft Windows Open Type Font Information Disclosure II (3199120)

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

Risk Level: Medium

CVE: CVE-2016-7256

Update Details

Recommendation is updated

20956 - (MS16-150) Microsoft Windows Secure Kernel Mode Privilege Escalation (3205642)

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

Risk Level: Medium

CVE: CVE-2016-7271

Update Details

Recommendation is updated

20961 - (MS16-146) Microsoft Windows GDI Information Disclosure (3204066)

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

Risk Level: Medium

CVE: CVE-2016-7257

Update Details

Recommendation is updated

20973 - (MS16-151) Microsoft Windows Win32k Privilege Escalation I (3205651)

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

Risk Level: Medium

CVE: CVE-2016-7259

Update Details

Recommendation is updated

20974 - (MS16-151) Microsoft Windows Win32k Privilege Escalation II (3205651)

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

Risk Level: Medium

CVE: CVE-2016-7260

Update Details

Recommendation is updated

20976 - (MS16-149) Microsoft Windows Crypto Driver Information Disclosure (3205655)

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

Risk Level: Medium
CVE: CVE-2016-7219

[Update Details](#)

Recommendation is updated

20977 - (MS16-149) Microsoft Windows Installer Privilege Escalation (3205655)

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

Risk Level: Medium
CVE: CVE-2016-7292

[Update Details](#)

Recommendation is updated

20983 - (MS16-145) Microsoft Edge Scripting Engine Remote Code Execution II (3204062)

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

Risk Level: Medium
CVE: CVE-2016-7286

[Update Details](#)

Recommendation is updated

20984 - (MS16-145) Microsoft Edge Memory Handling Information Disclosure (3204062)

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

Risk Level: Medium
CVE: CVE-2016-7282

[Update Details](#)

Recommendation is updated

20985 - (MS16-145) Microsoft Edge Browser Security Bypass (3204062)

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

Risk Level: Medium
CVE: CVE-2016-7281

[Update Details](#)

Recommendation is updated

20986 - (MS16-145) Microsoft Edge Memory Handling Information Disclosure II (3204062)

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

Risk Level: Medium
CVE: CVE-2016-7280

[Update Details](#)

Recommendation is updated

20988 - (MS16-145) Microsoft Edge Browser Information Disclosure I (3204062)

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

Risk Level: Medium

CVE: CVE-2016-7206

[Update Details](#)

Recommendation is updated

20989 - (MS16-145) Microsoft Edge Memory Handling Remote Code Execution I (3204062)

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

Risk Level: Medium

CVE: CVE-2016-7181

[Update Details](#)

Recommendation is updated

20990 - (MS16-152) Security Update for Windows Kernel (3199709)

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

Risk Level: Medium

CVE: CVE-2016-7258

[Update Details](#)

Recommendation is updated

20991 - (MS16-152) Microsoft Windows Kernel Memory Information Disclosure (3199709)

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

Risk Level: Medium

CVE: CVE-2016-7258

[Update Details](#)

Recommendation is updated

21006 - (MS16-153) Microsoft Windows Common Log File System Driver Privilege Escalation (3207328)

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

Risk Level: Medium

CVE: CVE-2016-7295

[Update Details](#)

Recommendation is updated

21008 - (MS16-153) Security Update for Common Log File System Driver (3207328)

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

Risk Level: Medium

CVE: CVE-2016-7295

Update Details

Recommendation is updated

21100 - (MS17-001) Microsoft Edge Privilege Escalation (3214288)

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

Risk Level: Medium

CVE: CVE-2017-0002

Update Details

Recommendation is updated

21335 - (MS17-017) Microsoft Windows Kernel Privilege Escalation (4013081)

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

Risk Level: Medium

CVE: CVE-2017-0050

Update Details

Recommendation is updated

21348 - (MS17-007) Microsoft Edge Browser Security Bypass II (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0135

Update Details

Recommendation is updated

21352 - (MS17-007) Microsoft Edge Memory Handling Same Origin Policy Security Bypass (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0140

Update Details

Recommendation is updated

21358 - (MS17-007) Microsoft Edge Spoofing Information Disclosure (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0069

Update Details

Recommendation is updated

21359 - (MS17-007) Microsoft Edge Browser Information Disclosure V (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0068

Update Details

Recommendation is updated

21361 - (MS17-007) Microsoft Edge Browser Security Bypass I (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0066

Update Details

Recommendation is updated

21362 - (MS17-007) Microsoft Edge Browser Information Disclosure IV (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0065

Update Details

Recommendation is updated

21367 - (MS17-007) Microsoft Edge Browser Information Disclosure III (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0033

Update Details

Recommendation is updated

21370 - (MS17-007) Microsoft Edge Memory Handling Information Disclosure II (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0017

Update Details

Recommendation is updated

21372 - (MS17-007) Microsoft Edge Browser Information Disclosure II (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0012

Update Details

Recommendation is updated

21373 - (MS17-007) Microsoft Edge Memory Handling Information Disclosure I (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0011

Update Details

Recommendation is updated

21375 - (MS17-007) Microsoft Edge Browser Information Disclosure I (4013071)

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

Risk Level: Medium

CVE: CVE-2017-0009

Update Details

Recommendation is updated

21446 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure I (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0085

Update Details

Recommendation is updated

21447 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure II (4013076)

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

Risk Level: Medium
CVE: CVE-2017-0091

[Update Details](#)

Recommendation is updated

21448 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure III (4013076)

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

Risk Level: Medium
CVE: CVE-2017-0111

[Update Details](#)

Recommendation is updated

21449 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure IV (4013076)

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

Risk Level: Medium
CVE: CVE-2017-0112

[Update Details](#)

Recommendation is updated

21450 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure V (4013076)

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

Risk Level: Medium
CVE: CVE-2017-0113

[Update Details](#)

Recommendation is updated

21451 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure VII (4013076)

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

Risk Level: Medium
CVE: CVE-2017-0115

[Update Details](#)

Recommendation is updated

21452 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure VI (4013076)

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

Risk Level: Medium
CVE: CVE-2017-0114

[Update Details](#)

Recommendation is updated

21453 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure VIII (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0116

[Update Details](#)

Recommendation is updated

21454 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure IX (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0119

[Update Details](#)

Recommendation is updated

21455 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure X (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0120

[Update Details](#)

Recommendation is updated

21456 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XI (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0122

[Update Details](#)

Recommendation is updated

21457 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XII (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0123

[Update Details](#)

Recommendation is updated

21458 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XIII (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0124

[Update Details](#)

Recommendation is updated

21459 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XIV (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0125

[Update Details](#)

Recommendation is updated

21460 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XV (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0126

[Update Details](#)

Recommendation is updated

21461 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XVI (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0127

[Update Details](#)

Recommendation is updated

21462 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XVII (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0128

[Update Details](#)

Recommendation is updated

21463 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XVIII (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0092

Update Details

Recommendation is updated

21464 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XIX (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0121

Update Details

Recommendation is updated

21465 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XX (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0117

Update Details

Recommendation is updated

21466 - (MS17-011) Microsoft Windows Uniscribe Information Disclosure XXI (4013076)

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

Risk Level: Medium

CVE: CVE-2017-0118

Update Details

Recommendation is updated

140917 - Red Hat Enterprise Linux RHSA-2015-1629 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0433, CVE-2015-0441, CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2582, CVE-2015-2620, CVE-2015-2643, CVE-2015-2648, CVE-2015-4737, CVE-2015-4752, CVE-2015-4757, CVE-2015-4816, CVE-2015-4819, CVE-2015-4864, CVE-2015-4879

Update Details

CVE is updated FASLScript is updated

140920 - Red Hat Enterprise Linux RHSA-2015-1657 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3900

Update Details

FASLScript is updated

140922 - Red Hat Enterprise Linux RHSA-2015-1665 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0433, CVE-2015-0441, CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2582, CVE-2015-2620, CVE-2015-2643, CVE-2015-2648, CVE-2015-3152, CVE-2015-4737, CVE-2015-4752, CVE-2015-4757, CVE-2015-4864

Update Details

CVE is updated

140924 - Red Hat Enterprise Linux RHSA-2015-1647 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0433, CVE-2015-0441, CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2582, CVE-2015-2620, CVE-2015-2643, CVE-2015-2648, CVE-2015-3152, CVE-2015-4737, CVE-2015-4752, CVE-2015-4757, CVE-2015-4864

Update Details

CVE is updated FASLScript is updated

140927 - Red Hat Enterprise Linux RHSA-2015-1666 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0228, CVE-2015-0253, CVE-2015-3183, CVE-2015-3185

Update Details

FASLScript is updated

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

Update Details

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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-2014-8182, CVE-2015-3276

Update Details

CVE is updated FASLScript is updated

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

Update Details

FASLScript is updated

141037 - Red Hat Enterprise Linux RHSA-2015-2617 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Update Details

FASLScript is updated

141043 - Red Hat Enterprise Linux RHSA-2015-2655 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Update Details

FASLScript is updated

141051 - Red Hat Enterprise Linux RHSA-2016-0006 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-7540

Update Details

FASLScript is updated

141053 - Red Hat Enterprise Linux RHSA-2016-0005 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7236

Update Details

FASLScript is updated

141055 - Red Hat Enterprise Linux RHSA-2016-0009 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3223, CVE-2015-5330

[Update Details](#)

FASLScript is updated

141067 - Red Hat Enterprise Linux RHSA-2016-0054 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4871, CVE-2015-7575, CVE-2016-0402, CVE-2016-0448, CVE-2016-0466, CVE-2016-0483, CVE-2016-0494

[Update Details](#)

FASLScript is updated

141069 - Red Hat Enterprise Linux RHSA-2016-0063 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8138

[Update Details](#)

FASLScript is updated

141097 - Red Hat Enterprise Linux RHSA-2016-0346 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0773

[Update Details](#)

FASLScript is updated

141098 - Red Hat Enterprise Linux RHSA-2016-0296 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7576, CVE-2015-7577, CVE-2015-7581, CVE-2016-0751, CVE-2016-0752, CVE-2016-0753

[Update Details](#)

FASLScript is updated

141099 - Red Hat Enterprise Linux RHSA-2016-0303 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0293, CVE-2015-3197, CVE-2016-0703, CVE-2016-0704, CVE-2016-0800

[Update Details](#)

FASLScript is updated

141104 - Red Hat Enterprise Linux RHSA-2016-0348 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0773

[Update Details](#)

FASLScript is updated

141105 - Red Hat Enterprise Linux RHSA-2016-0349 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0773

[Update Details](#)

FASLScript is updated

141111 - Red Hat Enterprise Linux RHSA-2016-0454 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7576, CVE-2015-7577, CVE-2015-7581, CVE-2016-0751, CVE-2016-0752, CVE-2016-2097, CVE-2016-2098

[Update Details](#)

FASLScript is updated

141114 - Red Hat Enterprise Linux RHSA-2016-0456 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0752, CVE-2016-2097, CVE-2016-2098

[Update Details](#)

FASLScript is updated

141120 - Red Hat Enterprise Linux RHSA-2016-0455 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7576, CVE-2015-7577, CVE-2016-0751, CVE-2016-0752, CVE-2016-2097, CVE-2016-2098

[Update Details](#)

FASLScript is updated

141126 - Red Hat Enterprise Linux RHSA-2016-0459 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

[Update Details](#)

FASLScript is updated

141129 - Red Hat Enterprise Linux RHSA-2016-0465 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1908, CVE-2016-3115

[Update Details](#)

FASLScript is updated

141143 - Red Hat Enterprise Linux RHSA-2016-0562 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

[Update Details](#)

FASLScript is updated

141144 - Red Hat Enterprise Linux RHSA-2016-0601 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

[Update Details](#)

FASLScript is updated

141200 - Red Hat Enterprise Linux RHSA-2016-1166 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2099, CVE-2013-7440, CVE-2014-9365

[Update Details](#)

FASLScript is updated

141218 - Red Hat Enterprise Linux RHSA-2016-1380 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7191

[Update Details](#)

FASLScript is updated

141221 - Red Hat Enterprise Linux RHSA-2016-1420 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4979, CVE-2016-5387

Update Details

FASLScript is updated

141224 - Red Hat Enterprise Linux RHSA-2016-1422 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5387

Update Details

FASLScript is updated

141237 - Red Hat Enterprise Linux RHSA-2016-1538 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741, CVE-2016-3959, CVE-2016-5386

Update Details

CVE is updated

141246 - Red Hat Enterprise Linux RHSA-2016-1610 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5385

Update Details

FASLScript is updated

141247 - Red Hat Enterprise Linux RHSA-2016-1613 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5385

Update Details

FASLScript is updated

141250 - Red Hat Enterprise Linux RHSA-2016-1612 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5385

[Update Details](#)

FASLScript is updated

141255 - Red Hat Enterprise Linux RHSA-2016-1611 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5385

[Update Details](#)

FASLScript is updated

141260 - Red Hat Enterprise Linux RHSA-2016-1626 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699

[Update Details](#)

FASLScript is updated

141263 - Red Hat Enterprise Linux RHSA-2016-1627 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699

[Update Details](#)

FASLScript is updated

141264 - Red Hat Enterprise Linux RHSA-2016-1630 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699

[Update Details](#)

FASLScript is updated

141266 - Red Hat Enterprise Linux RHSA-2016-1633 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5696

[Update Details](#)

FASLScript is updated

141267 - Red Hat Enterprise Linux RHSA-2016-1629 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699

[Update Details](#)

FASLScript is updated

141268 - Red Hat Enterprise Linux RHSA-2016-1628 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699

[Update Details](#)

FASLScript is updated

141281 - Red Hat Enterprise Linux RHSA-2016-1855 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6316, CVE-2016-6317

[Update Details](#)

FASLScript is updated

141320 - Red Hat Enterprise Linux RHSA-2016-2575 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5419, CVE-2016-5420, CVE-2016-7141

[Update Details](#)

FASLScript is updated

141324 - Red Hat Enterprise Linux RHSA-2016-2592 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4455

[Update Details](#)

FASLScript is updated

141326 - Red Hat Enterprise Linux RHSA-2016-2674 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

[Update Details](#)

FASLScript is updated

141332 - Red Hat Enterprise Linux RHSA-2016-2594 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4992, CVE-2016-5405, CVE-2016-5416

Update Details

FASLScript is updated

141334 - Red Hat Enterprise Linux RHSA-2016-2615 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Update Details

FASLScript is updated

141336 - Red Hat Enterprise Linux RHSA-2016-2603 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5361

Update Details

FASLScript is updated

141348 - Red Hat Enterprise Linux RHSA-2016-2583 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7974, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8158

Update Details

FASLScript is updated

141356 - Red Hat Enterprise Linux RHSA-2016-2600 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-2572, CVE-2016-3948

Update Details

FASLScript is updated

141377 - Red Hat Enterprise Linux RHSA-2016-2872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

[Update Details](#)

FASLScript is updated

141378 - Red Hat Enterprise Linux RHSA-2016-2871 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

[Update Details](#)

FASLScript is updated

191757 - Fedora Linux 24 FEDORA-2017-a8dc348834 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6004

[Update Details](#)

Risk 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

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

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

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

19358 - (MS15-124) Microsoft Internet Explorer XSS Filter Security Bypass I (3116180)

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

Risk Level: Medium

CVE: CVE-2015-6138

[Update Details](#)

Recommendation is updated

19364 - (MS15-124) Microsoft Internet Explorer XSS Filter Security Bypass II (3116180)

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

Risk Level: Medium

CVE: CVE-2015-6144

[Update Details](#)

Recommendation is updated

19377 - (MS15-124) Microsoft Internet Explorer Memory Content Information Disclosure (3116180)

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

Risk Level: Medium

CVE: CVE-2015-6157

[Update Details](#)

Recommendation is updated

19381 - (MS15-124) Microsoft Internet Explorer ASLR Security Bypass (3116180)

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

Risk Level: Medium

CVE: CVE-2015-6161

[Update Details](#)

Recommendation is updated

20022 - (MS16-065) Microsoft .NET Framework Encryption TLS/SSL Information Disclosure (3156757)

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

Risk Level: Medium

CVE: CVE-2016-0149

[Update Details](#)

Recommendation is updated

20023 - (MS16-065) Security Update for .NET Framework (3156757)

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

Risk Level: Medium

CVE: CVE-2016-0149

[Update Details](#)

Recommendation is updated

20302 - (MS16-085) Microsoft Edge Scripting Engine Information Disclosure (3169999)

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

Risk Level: Medium

CVE: CVE-2016-3271

Update Details

Recommendation is updated

20310 - (MS16-085) Microsoft Edge Security Bypass (3169999)

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

Risk Level: Medium

CVE: CVE-2016-3244

Update Details

Recommendation is updated

20395 - (MS16-103) Security Update for ActiveSyncProvider (3182332)

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

Risk Level: Medium

CVE: CVE-2016-3312

Update Details

Recommendation is updated

20630 - (MS16-119) Microsoft Edge Browser Information Disclosure I (3192890)

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

Risk Level: Medium

CVE: CVE-2016-3267

Update Details

Recommendation is updated

20647 - (MS16-124) Security Update for Windows Registry (3193227)

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

Risk Level: Medium

CVE: CVE-2016-0070, CVE-2016-0073, CVE-2016-0075, CVE-2016-0079

Update Details

Recommendation is updated

20651 - (MS16-124) Microsoft Windows Kernel Privilege Escalation I (3193227)

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

Risk Level: Medium

CVE: CVE-2016-0070

[Update Details](#)

Recommendation is updated

140852 - Red Hat Enterprise Linux RHSA-2015-1185 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2721, CVE-2015-4000

[Update Details](#)

CVE is updated

140853 - Red Hat Enterprise Linux RHSA-2015-1195 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3165, CVE-2015-3166, CVE-2015-3167

[Update Details](#)

FASLScript is updated

140855 - Red Hat Enterprise Linux RHSA-2015-1196 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3165, CVE-2015-3166, CVE-2015-3167

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

141028 - Red Hat Enterprise Linux RHSA-2015-2552 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

[Update Details](#)

FASLScript is updated

141056 - Red Hat Enterprise Linux RHSA-2016-0012 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7575

[Update Details](#)

FASLScript is updated

141058 - Red Hat Enterprise Linux RHSA-2016-0007 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7575

[Update Details](#)

FASLScript is updated

141059 - Red Hat Enterprise Linux RHSA-2016-0008 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7575

[Update Details](#)

FASLScript is updated

141061 - Red Hat Enterprise Linux RHSA-2016-0043 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0777, CVE-2016-0778

[Update Details](#)

FASLScript is updated

141064 - Red Hat Enterprise Linux RHSA-2016-0049 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7575, CVE-2016-0402, CVE-2016-0448, CVE-2016-0466, CVE-2016-0475, CVE-2016-0483, CVE-2016-0494

[Update Details](#)

FASLScript is updated

141091 - Red Hat Enterprise Linux RHSA-2016-0189 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3256

[Update Details](#)

FASLScript is updated

141106 - Red Hat Enterprise Linux RHSA-2016-0305 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3197, CVE-2016-0800

[Update Details](#)

FASLScript is updated

141115 - Red Hat Enterprise Linux RHSA-2016-0428 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0787

[Update Details](#)

FASLScript is updated

141121 - Red Hat Enterprise Linux RHSA-2016-0448 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7560

[Update Details](#)

FASLScript is updated

141151 - Red Hat Enterprise Linux RHSA-2016-0619 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

[Update Details](#)

FASLScript is updated

141157 - Red Hat Enterprise Linux RHSA-2016-0612 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

[Update Details](#)

FASLScript is updated

141159 - Red Hat Enterprise Linux RHSA-2016-0620 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

[Update Details](#)

FASLScript is updated

141257 - Red Hat Enterprise Linux RHSA-2016-1606 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5126, CVE-2016-5403

[Update Details](#)

FASLScript is updated

141271 - Red Hat Enterprise Linux RHSA-2016-1797 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5404

[Update Details](#)

FASLScript is updated

141278 - Red Hat Enterprise Linux RHSA-2016-1857 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6316

[Update Details](#)

FASLScript is updated

141279 - Red Hat Enterprise Linux RHSA-2016-1858 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6316

[Update Details](#)

FASLScript is updated

141280 - Red Hat Enterprise Linux RHSA-2016-1856 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6316

[Update Details](#)

FASLScript is updated

141329 - Red Hat Enterprise Linux RHSA-2016-2577 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5160, CVE-2015-5313, CVE-2016-5008

[Update Details](#)

FASLScript is updated

141330 - Red Hat Enterprise Linux RHSA-2016-2587 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4971

[Update Details](#)

FASLScript is updated

141343 - Red Hat Enterprise Linux RHSA-2016-2601 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5384

[Update Details](#)

FASLScript is updated

141346 - Red Hat Enterprise Linux RHSA-2016-2591 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-3119, CVE-2016-3120

[Update Details](#)

FASLScript is updated

141353 - Red Hat Enterprise Linux RHSA-2016-2593 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium
CVE: CVE-2016-7091

[Update Details](#)

FASLScript is updated

141354 - Red Hat Enterprise Linux RHSA-2016-2610 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-7795

[Update Details](#)

FASLScript is updated

182270 - FreeBSD mysql Multiple Vulnerabilities (4d2f9d09-ddb7-11e6-a9a5-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8318, CVE-2016-8327, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3251, CVE-2017-3256, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3273, CVE-2017-3291, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3319, CVE-2017-3320

[Update Details](#)

FASLScript is updated

20758 - (MS16-138) Security Update to Microsoft Virtual Hard Drive (3199647)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-7223, CVE-2016-7224, CVE-2016-7225, CVE-2016-7226

[Update Details](#)

Recommendation is updated

31623 - Oracle Solaris 125719-57 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, CVE-2011-4028, CVE-2013-4396, CVE-2014-0209, CVE-2014-0210, CVE-2014-0211

[Update Details](#)

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33319 - Oracle Solaris 151913-09 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

33323 - Oracle Solaris 151912-09 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

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

141333 - Red Hat Enterprise Linux RHSA-2016-2605 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-5011

[Update Details](#)

FASLScript is updated

141345 - Red Hat Enterprise Linux RHSA-2016-2602 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-3099

[Update Details](#)

FASLScript is updated

141350 - Red Hat Enterprise Linux RHSA-2016-2581 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-0764

Update Details

FASLScript 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

20024 - (MS16-066) Microsoft Windows Hypervisor Code Integrity Security Bypass (3155451)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0181

[Update Details](#)

Recommendation is updated

20025 - (MS16-066) Security Update for Virtual Secure Mode (3155451)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0181

[Update Details](#)

Recommendation is updated

20275 - (MS16-092) Security Update for Windows Kernel (3171910)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3258, CVE-2016-3272

[Update Details](#)

Recommendation is updated

20276 - (MS16-092) Microsoft Windows Kernel Information Disclosure (3171910)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3272

[Update Details](#)

Recommendation is updated

20299 - (MS16-085) Microsoft Edge Browser Spoofing II (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3276

[Update Details](#)

Recommendation is updated

20300 - (MS16-085) Microsoft Edge Browser Spoofing I (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3274

[Update Details](#)

Recommendation is updated

20301 - (MS16-085) Microsoft Edge Browser Information Disclosure (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3273

[Update Details](#)

Recommendation is updated

20308 - (MS16-085) Microsoft Edge Memory Corruption Remote Code Execution III (3169999)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3277

[Update Details](#)

Recommendation is updated

20311 - (MS16-089) Security Update for Windows Secure Kernel Mode (3170050)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3256

[Update Details](#)

Recommendation is updated

20312 - (MS16-089) Microsoft Windows Secure Kernel Information Disclosure (3170050)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3256

[Update Details](#)

Recommendation is updated

20625 - (MS16-119) Microsoft Edge Browser Security Bypass (3192890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3392

[Update Details](#)

Recommendation is updated

20627 - (MS16-119) Microsoft Edge Browser Privilege Escalation I (3192890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3388

Update Details

Recommendation is updated

20629 - (MS16-119) Microsoft Edge Browser Credential Data Information Disclosure (3192890)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3391

Update Details

Recommendation is updated

20648 - (MS16-124) Microsoft Windows Kernel Privilege Escalation IV (3193227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0079

Update Details

Recommendation is updated

20649 - (MS16-124) Microsoft Windows Kernel Privilege Escalation III (3193227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0075

Update Details

Recommendation is updated

20650 - (MS16-124) Microsoft Windows Kernel Privilege Escalation II (3193227)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0073

Update Details

Recommendation is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

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

[Update Details](#)

FASLScript is updated

141321 - Red Hat Enterprise Linux RHSA-2016-2585 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-1981, CVE-2016-3712

[Update Details](#)

FASLScript is updated

191237 - Fedora Linux 25 FEDORA-2016-39de4eb5e7 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-7553

[Update Details](#)

Risk is updated

20277 - (MS16-092) Microsoft Windows File System Security Feature Security Bypass (3171910)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3258

[Update Details](#)

Recommendation is updated

45001 - ShellInitialize.fasl3

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70041 - rpm.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-2001-0923

Update Details

FASLScript is updated

DELETED CHECKS

21001 - (MS16-148) Microsoft Office Memory Corruption Remote Code Execution IV (3204068)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-7274

ADDITIONAL NOTES

- **21001** - is replaced by FID 21512.

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.

MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com/>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2017 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates