2016-NOV-03
FSL version 7.5.862

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

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-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

Description

The scan detected that the host is missing the following update:
RHSA-2016-2131

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2131.html

RHEL6_6S
x86_64
mariadb55-mariadb-libs-5.5.53-1.el6
mariadb55-mariadb-bench-5.5.53-1.el6
mariadb55-mariadb-devel-5.5.53-1.el6
mariadb55-mariadb-5.5.53-1.el6
mariadb55-mariadb-debuginfo-5.5.53-1.el6
mariadb55-mariadb-test-5.5.53-1.el6
mariadb55-mariadb-server-5.5.53-1.el6

RHEL6S
x86_64
mariadb55-mariadb-libs-5.5.53-1.el6
mariadb55-mariadb-bench-5.5.53-1.el6
mariadb55-mariadb-devel-5.5.53-1.el6
mariadb55-mariadb-5.5.53-1.el6
mariadb55-mariadb-debuginfo-5.5.53-1.el6
mariadb55-mariadb-test-5.5.53-1.el6
mariadb55-mariadb-server-5.5.53-1.el6

RHEL6WS
x86_64
mariadb55-mariadb-libs-5.5.53-1.el6
mariadb55-mariadb-bench-5.5.53-1.el6
mariadb55-mariadb-devel-5.5.53-1.el6
mariadb55-mariadb-5.5.53-1.el6
mariadb55-mariadb-debuginfo-5.5.53-1.el6
mariadb55-mariadb-test-5.5.53-1.el6
mariadb55-mariadb-server-5.5.53-1.el6

RHEL7S
x86_64
mariadb55-mariadb-libs-5.5.53-1.el7
mariadb55-mariadb-debuginfo-5.5.53-1.el7
mariadb55-mariadb-5.5.53-1.el7
mariadb55-mariadb-test-5.5.53-1.el7
mariadb55-mariadb-bench-5.5.53-1.el7
mariadb55-mariadb-server-5.5.53-1.el7
mariadb55-mariadb-devel-5.5.53-1.el7

RHEL7WS
x86_64
mariadb55-mariadb-libs-5.5.53-1.el7
mariadb55-mariadb-debuginfo-5.5.53-1.el7
mariadb55-mariadb-5.5.53-1.el7
mariadb55-mariadb-test-5.5.53-1.el7
mariadb55-mariadb-bench-5.5.53-1.el7
mariadb55-mariadb-server-5.5.53-1.el7
mariadb55-mariadb-devel-5.5.53-1.el7

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-2016-5616, CVE-2016-5617, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-8283

Description

The scan detected that the host is missing the following update:
RHSA-2016-2130

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2130.html

RHEL6_6S
x86_64
mysql55-mysql-test-5.5.52-1.el6
mysql55-mysql-libs-5.5.52-1.el6
mysql55-mysql-server-5.5.52-1.el6
mysql55-mysql-bench-5.5.52-1.el6
mysql55-mysql-debuginfo-5.5.52-1.el6
mysql55-mysql-devel-5.5.52-1.el6
mysql55-mysql-5.5.52-1.el6

RHEL6S
x86_64
mysql55-mysql-test-5.5.52-1.el6
mysql55-mysql-libs-5.5.52-1.el6
mysql55-mysql-server-5.5.52-1.el6
mysql55-mysql-bench-5.5.52-1.el6
mysql55-mysql-debuginfo-5.5.52-1.el6
mysql55-mysql-devel-5.5.52-1.el6
mysql55-mysql-5.5.52-1.el6

RHEL6WS

x86_64
mysql55-mysql-test-5.5.52-1.el6
mysql55-mysql-libs-5.5.52-1.el6
mysql55-mysql-server-5.5.52-1.el6
mysql55-mysql-bench-5.5.52-1.el6
mysql55-mysql-debuginfo-5.5.52-1.el6
mysql55-mysql-devel-5.5.52-1.el6
mysql55-mysql-5.5.52-1.el6

RHEL7S
x86_64
mysql55-mysql-libs-5.5.52-1.el7
mysql55-mysql-debuginfo-5.5.52-1.el7
mysql55-mysql-5.5.52-1.el7
mysql55-mysql-server-5.5.52-1.el7
mysql55-mysql-bench-5.5.52-1.el7
mysql55-mysql-test-5.5.52-1.el7
mysql55-mysql-devel-5.5.52-1.el7

RHEL7WS
x86_64
mysql55-mysql-libs-5.5.52-1.el7
mysql55-mysql-debuginfo-5.5.52-1.el7
mysql55-mysql-5.5.52-1.el7
mysql55-mysql-server-5.5.52-1.el7
mysql55-mysql-bench-5.5.52-1.el7
mysql55-mysql-test-5.5.52-1.el7
mysql55-mysql-devel-5.5.52-1.el7

178232 - Gentoo Linux GLSA-201610-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4182, CVE-2016-4271, CVE-2016-4272, CVE-2016-4273, CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4277, CVE-2016-4278, CVE-2016-4279, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-4286, CVE-2016-4287, CVE-2016-6921, CVE-2016-6922, CVE-2016-6923, CVE-2016-6924, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, CVE-2016-6932, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE-2016-6990, CVE-2016-6992, CVE-2016-7855

Description

The scan detected that the host is missing the following update:
GLSA-201610-10

Observation

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

https://security.gentoo.org/glsa/201610-10

Affected packages:
www-plugins/adobe-flash < 23.0.0.205

20749 - Microsoft Windows NtSetWindowLongPtr Privilege Escalation

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in NtSetWindowLongPtr(). Successful exploitation could allow a local user to gain elevated privileges.

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2136

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2136.html

RHEL7S
ppc64
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el7_2

RHEL6S
i386
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el6_8

x86_64
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el6_8

RHEL6WS
x86_64
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el6_8

java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el6_8

i386
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el6_8

RHEL7D
x86_64
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el7_2

RHEL6D
x86_64
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el6_8

i386
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el6_8
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el6_8

RHEL7WS
x86_64
java-1.8.0-ibm-devel-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-demo-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-jdbc-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-src-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-plugin-1.8.0.3.20-1jpp.1.el7_2
java-1.8.0-ibm-1.8.0.3.20-1jpp.1.el7_2

141314 - Red Hat Enterprise Linux RHSA-2016-2138 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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2138

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2138.html

RHEL5D
x86_64
java-1.7.0-ibm-jdbc-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-demo-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-src-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-devel-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-plugin-1.7.0.9.60-1jpp.1.el5_11

i386
java-1.7.0-ibm-jdbc-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-demo-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-src-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-devel-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-plugin-1.7.0.9.60-1jpp.1.el5_11

RHEL5S
i386
java-1.7.0-ibm-jdbc-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-demo-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-src-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-devel-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-plugin-1.7.0.9.60-1jpp.1.el5_11

x86_64
java-1.7.0-ibm-jdbc-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-demo-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-src-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-devel-1.7.0.9.60-1jpp.1.el5_11
java-1.7.0-ibm-plugin-1.7.0.9.60-1jpp.1.el5_11

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2137

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2137.html

RHEL7S
ppc64

java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el7_2

RHEL6S
i386
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el6_8

x86_64
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el6_8

RHEL6WS
x86_64
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el6_8

i386
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el6_8

RHEL7D
x86_64
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el7_2

RHEL6D
x86_64
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el6_8

i386

java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el6_8
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el6_8

RHEL7WS
x86_64
java-1.7.1-ibm-src-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-devel-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-demo-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-plugin-1.7.1.3.60-1jpp.1.el7_2
java-1.7.1-ibm-jdbc-1.7.1.3.60-1jpp.1.el7_2

144973 - SuSE Linux 13.2 openSUSE-SU-2016:2672-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8540

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2672-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00108.html

SuSE Linux 13.2
x86_64
libpng12-compat-devel-32bit-1.2.51-3.9.1
libpng12-0-32bit-1.2.51-3.9.1
libpng12-0-1.2.51-3.9.1
libpng12-debugsource-1.2.51-3.9.1
libpng12-devel-1.2.51-3.9.1
libpng12-0-debuginfo-32bit-1.2.51-3.9.1
libpng12-0-debuginfo-1.2.51-3.9.1
libpng12-compat-devel-1.2.51-3.9.1
libpng12-devel-32bit-1.2.51-3.9.1

i586
libpng12-debugsource-1.2.51-3.9.1
libpng12-0-debuginfo-1.2.51-3.9.1
libpng12-0-1.2.51-3.9.1
libpng12-devel-1.2.51-3.9.1
libpng12-compat-devel-1.2.51-3.9.1

132292 - Oracle VM OVMSA-2016-0151 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-5485

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0151

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000572.html
http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000571.html

OVM3.3
x86_64
ovm-consoled-0.1-17.el6.0.1

OVM3.4
x86_64
ovm-consoled-0.1-20.el6.2

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2132

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2132.html

RHEL6_2S
x86_64
python-perf-debuginfo-2.6.32-220.68.1.el6
perf-debuginfo-2.6.32-220.68.1.el6
kernel-debuginfo-2.6.32-220.68.1.el6
kernel-debug-debuginfo-2.6.32-220.68.1.el6
python-perf-2.6.32-220.68.1.el6
kernel-debuginfo-common-x86_64-2.6.32-220.68.1.el6

144968 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2668-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-7568, CVE-2016-8670

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2668-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002374.html

SuSE SLES 12 SP1
x86_64
gd-2.1.0-17.1
gd-debugsource-2.1.0-17.1
gd-debuginfo-2.1.0-17.1

SuSE SLED 12 SP1
x86_64
gd-32bit-2.1.0-17.1
gd-debuginfo-32bit-2.1.0-17.1
gd-2.1.0-17.1
gd-debugsource-2.1.0-17.1
gd-debuginfo-2.1.0-17.1

144969 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2667-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9907, CVE-2015-8957, CVE-2015-8958, CVE-2015-8959, CVE-2016-6823, CVE-2016-7101, CVE-2016-7513, CVE-2016-7514, CVE-2016-7515, CVE-2016-7516, CVE-2016-7517, CVE-2016-7518, CVE-2016-7519, CVE-2016-7520, CVE-2016-7521, CVE-2016-7522, CVE-2016-7523, CVE-2016-7524, CVE-2016-7525, CVE-2016-7526, CVE-2016-7527, CVE-2016-7528, CVE-2016-7529, CVE-2016-7530, CVE-2016-7531, CVE-2016-7532, CVE-2016-7533, CVE-2016-7534, CVE-2016-7535, CVE-2016-7537, CVE-2016-7538, CVE-2016-7539, CVE-2016-7540, CVE-2016-7799, CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8677, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2667-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002373.html

SuSE SLES 12 SP1
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-40.1
libMagickCore-6_Q16-1-6.8.8.1-40.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-40.1
ImageMagick-debuginfo-6.8.8.1-40.1
ImageMagick-debugsource-6.8.8.1-40.1
libMagickWand-6_Q16-1-6.8.8.1-40.1

SuSE SLED 12 SP1
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-40.1
libMagick++-6_Q16-3-6.8.8.1-40.1
libMagickCore-6_Q16-1-6.8.8.1-40.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-40.1
ImageMagick-6.8.8.1-40.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-40.1
ImageMagick-debuginfo-6.8.8.1-40.1

ImageMagick-debugsource-6.8.8.1-40.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-40.1
libMagickWand-6_Q16-1-6.8.8.1-40.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-40.1

144970 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2697-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2697-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002385.html

SuSE SLED 12 SP1
x86_64
bind-libs-9.9.9P1-49.1
bind-libs-32bit-9.9.9P1-49.1
bind-libs-debuginfo-32bit-9.9.9P1-49.1
bind-utils-9.9.9P1-49.1
bind-debugsource-9.9.9P1-49.1
bind-debuginfo-9.9.9P1-49.1
bind-utils-debuginfo-9.9.9P1-49.1
bind-libs-debuginfo-9.9.9P1-49.1

SuSE SLES 12 SP2
noarch
bind-doc-9.9.9P1-49.1

x86_64
bind-debuginfo-9.9.9P1-49.1
bind-libs-9.9.9P1-49.1
bind-libs-32bit-9.9.9P1-49.1
bind-libs-debuginfo-32bit-9.9.9P1-49.1
bind-utils-9.9.9P1-49.1
bind-debugsource-9.9.9P1-49.1
bind-chrootenv-9.9.9P1-49.1
bind-9.9.9P1-49.1
bind-utils-debuginfo-9.9.9P1-49.1
bind-libs-debuginfo-9.9.9P1-49.1

SuSE SLED 12 SP2
x86_64
bind-libs-9.9.9P1-49.1
bind-libs-32bit-9.9.9P1-49.1
bind-libs-debuginfo-32bit-9.9.9P1-49.1
bind-utils-9.9.9P1-49.1
bind-debugsource-9.9.9P1-49.1
bind-debuginfo-9.9.9P1-49.1
bind-utils-debuginfo-9.9.9P1-49.1
bind-libs-debuginfo-9.9.9P1-49.1

SuSE SLES 12 SP1
noarch
bind-doc-9.9.9P1-49.1

x86_64
bind-debuginfo-9.9.9P1-49.1
bind-libs-9.9.9P1-49.1
bind-libs-32bit-9.9.9P1-49.1
bind-libs-debuginfo-32bit-9.9.9P1-49.1
bind-utils-9.9.9P1-49.1
bind-debugsource-9.9.9P1-49.1
bind-chrootenv-9.9.9P1-49.1
bind-9.9.9P1-49.1
bind-utils-debuginfo-9.9.9P1-49.1
bind-libs-debuginfo-9.9.9P1-49.1

144971 - SuSE SLES 11 SP4 SUSE-SU-2016:2681-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-8670

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2681-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002378.html

SuSE SLES 11 SP4
i586
php53-pear-5.3.17-87.1
php53-curl-5.3.17-87.1
php53-dom-5.3.17-87.1
php53-calendar-5.3.17-87.1
php53-exif-5.3.17-87.1
php53-gd-5.3.17-87.1
php53-snmp-5.3.17-87.1
php53-mbstring-5.3.17-87.1
php53-zip-5.3.17-87.1
php53-bz2-5.3.17-87.1
php53-soap-5.3.17-87.1
php53-mcrypt-5.3.17-87.1
apache2-mod_php53-5.3.17-87.1
php53-dba-5.3.17-87.1
php53-gmp-5.3.17-87.1
php53-odbc-5.3.17-87.1
php53-mysql-5.3.17-87.1
php53-openssl-5.3.17-87.1
php53-sysvmsg-5.3.17-87.1
php53-pgsql-5.3.17-87.1
php53-ctype-5.3.17-87.1
php53-suhosin-5.3.17-87.1
php53-intl-5.3.17-87.1
php53-gettext-5.3.17-87.1

php53-pcntl-5.3.17-87.1
php53-tokenizer-5.3.17-87.1
php53-xmlrpc-5.3.17-87.1
php53-pspell-5.3.17-87.1
php53-ftp-5.3.17-87.1
php53-pdo-5.3.17-87.1
php53-ldap-5.3.17-87.1
php53-json-5.3.17-87.1
php53-zlib-5.3.17-87.1
php53-wddx-5.3.17-87.1
php53-5.3.17-87.1
php53-xsl-5.3.17-87.1
php53-fastcgi-5.3.17-87.1
php53-fileinfo-5.3.17-87.1
php53-xmlreader-5.3.17-87.1
php53-sysvsem-5.3.17-87.1
php53-iconv-5.3.17-87.1
php53-xmlwriter-5.3.17-87.1
php53-sysvshm-5.3.17-87.1
php53-bcmath-5.3.17-87.1
php53-shmop-5.3.17-87.1

x86_64
php53-pear-5.3.17-87.1
php53-curl-5.3.17-87.1
php53-dom-5.3.17-87.1
php53-calendar-5.3.17-87.1
php53-exif-5.3.17-87.1
php53-gd-5.3.17-87.1
php53-snmp-5.3.17-87.1
php53-mbstring-5.3.17-87.1
php53-zip-5.3.17-87.1
php53-bz2-5.3.17-87.1
php53-soap-5.3.17-87.1
php53-mcrypt-5.3.17-87.1
apache2-mod_php53-5.3.17-87.1
php53-dba-5.3.17-87.1
php53-gmp-5.3.17-87.1
php53-odbc-5.3.17-87.1
php53-mysql-5.3.17-87.1
php53-openssl-5.3.17-87.1
php53-sysvmsg-5.3.17-87.1
php53-pgsql-5.3.17-87.1
php53-ctype-5.3.17-87.1
php53-suhosin-5.3.17-87.1
php53-intl-5.3.17-87.1
php53-gettext-5.3.17-87.1
php53-pcntl-5.3.17-87.1
php53-tokenizer-5.3.17-87.1
php53-xmlrpc-5.3.17-87.1
php53-pspell-5.3.17-87.1
php53-ftp-5.3.17-87.1
php53-pdo-5.3.17-87.1
php53-ldap-5.3.17-87.1
php53-json-5.3.17-87.1
php53-zlib-5.3.17-87.1
php53-wddx-5.3.17-87.1
php53-5.3.17-87.1
php53-xsl-5.3.17-87.1
php53-fastcgi-5.3.17-87.1

php53-fileinfo-5.3.17-87.1
php53-xmlreader-5.3.17-87.1
php53-sysvsem-5.3.17-87.1
php53-iconv-5.3.17-87.1
php53-xmlwriter-5.3.17-87.1
php53-sysvshm-5.3.17-87.1
php53-bcmath-5.3.17-87.1
php53-shmop-5.3.17-87.1

144972 - SuSE Linux 13.2 openSUSE-SU-2016:2671-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9907, CVE-2015-8957, CVE-2015-8958, CVE-2015-8959, CVE-2016-6823, CVE-2016-7101, CVE-2016-7513, CVE-2016-7514, CVE-2016-7515, CVE-2016-7516, CVE-2016-7517, CVE-2016-7518, CVE-2016-7519, CVE-2016-7520, CVE-2016-7521, CVE-2016-7522, CVE-2016-7523, CVE-2016-7524, CVE-2016-7525, CVE-2016-7527, CVE-2016-7528, CVE-2016-7529, CVE-2016-7530, CVE-2016-7531, CVE-2016-7532, CVE-2016-7533, CVE-2016-7534, CVE-2016-7535, CVE-2016-7536, CVE-2016-7537, CVE-2016-7538, CVE-2016-7539, CVE-2016-7540, CVE-2016-7799, CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8677, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2671-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00107.html

SuSE Linux 13.2
i586
libMagick++-6_Q16-5-6.8.9.8-34.1
libMagickWand-6_Q16-2-6.8.9.8-34.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-34.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-34.1
perl-PerlMagick-debuginfo-6.8.9.8-34.1
ImageMagick-extra-debuginfo-6.8.9.8-34.1
ImageMagick-debugsource-6.8.9.8-34.1
ImageMagick-6.8.9.8-34.1
libMagickCore-6_Q16-2-6.8.9.8-34.1
libMagick++-devel-6.8.9.8-34.1
ImageMagick-devel-6.8.9.8-34.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-34.1
ImageMagick-extra-6.8.9.8-34.1
ImageMagick-debuginfo-6.8.9.8-34.1
perl-PerlMagick-6.8.9.8-34.1

noarch
ImageMagick-doc-6.8.9.8-34.1

x86_64
libMagick++-6_Q16-5-6.8.9.8-34.1
libMagickWand-6_Q16-2-6.8.9.8-34.1
libMagickWand-6_Q16-2-32bit-6.8.9.8-34.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-34.1
libMagickCore-6_Q16-2-debuginfo-32bit-6.8.9.8-34.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-34.1

perl-PerlMagick-debuginfo-6.8.9.8-34.1
ImageMagick-extra-debuginfo-6.8.9.8-34.1
ImageMagick-debugsource-6.8.9.8-34.1
ImageMagick-6.8.9.8-34.1
libMagickCore-6_Q16-2-6.8.9.8-34.1
libMagickCore-6_Q16-2-32bit-6.8.9.8-34.1
libMagickWand-6_Q16-2-debuginfo-32bit-6.8.9.8-34.1
libMagick++-6_Q16-5-debuginfo-32bit-6.8.9.8-34.1
libMagick++-devel-6.8.9.8-34.1
ImageMagick-devel-6.8.9.8-34.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-34.1
ImageMagick-devel-32bit-6.8.9.8-34.1
ImageMagick-extra-6.8.9.8-34.1
ImageMagick-debuginfo-6.8.9.8-34.1
libMagick++-6_Q16-5-32bit-6.8.9.8-34.1
perl-PerlMagick-6.8.9.8-34.1
libMagick++-devel-32bit-6.8.9.8-34.1

144974 - SuSE SLES 11 SP4 SUSE-SU-2016:2670-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-8670

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2670-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002375.html

SuSE SLES 11 SP4
i586
gd-2.0.36.RC1-52.25.1

x86_64
gd-2.0.36.RC1-52.25.1

160162 - CentOS 5 CESA-2016-2124 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-5195

Description

The scan detected that the host is missing the following update:
CESA-2016-2124

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-October/022135.html

CentOS 5
i386
kernel-headers-2.6.18-416.el5

i686
kernel-PAE-2.6.18-416.el5
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-PAE-devel-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-2.6.18-416.el5

noarch
kernel-doc-2.6.18-416.el5

x86_64
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-headers-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-2.6.18-416.el5

163181 - Oracle Enterprise Linux ELSA-2016-2124 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-5195

Description

The scan detected that the host is missing the following update:
ELSA-2016-2124

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006449.html
http://oss.oracle.com/pipermail/el-errata/2016-October/006447.html

OEL5
i386
kernel-PAE-2.6.18-416.0.0.0.1.el5
kernel-2.6.18-416.el5
kernel-2.6.18-416.0.0.0.1.el5
kernel-devel-2.6.18-416.0.0.0.1.el5
kernel-PAE-devel-2.6.18-416.el5
kernel-doc-2.6.18-416.0.0.0.1.el5
kernel-debug-2.6.18-416.0.0.0.1.el5
kernel-debug-2.6.18-416.el5
kernel-PAE-devel-2.6.18-416.0.0.0.1.el5
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.0.0.0.1.el5
kernel-PAE-2.6.18-416.el5

kernel-headers-2.6.18-416.0.0.0.1.el5
kernel-devel-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.0.0.0.1.el5
kernel-doc-2.6.18-416.el5
kernel-headers-2.6.18-416.el5
kernel-xen-2.6.18-416.0.0.0.1.el5

x86_64
kernel-2.6.18-416.el5
kernel-2.6.18-416.0.0.0.1.el5
kernel-doc-2.6.18-416.0.0.0.1.el5
kernel-debug-2.6.18-416.0.0.0.1.el5
kernel-debug-2.6.18-416.el5
kernel-devel-2.6.18-416.0.0.0.1.el5
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.0.0.0.1.el5
kernel-headers-2.6.18-416.0.0.0.1.el5
kernel-devel-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.0.0.0.1.el5
kernel-doc-2.6.18-416.el5
kernel-headers-2.6.18-416.el5
kernel-xen-2.6.18-416.0.0.0.1.el5

175028 - Scientific Linux Security ERRATA Important: kernel on SL5.x i386/x86_64 (1610-6706)

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-5195

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL5.x i386/x86_64 (1610-6706)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1610&L=scientific-linux-errata&F=&S=&P=6706

SL5
i386
kernel-2.6.18-416.el5
kernel-debuginfo-2.6.18-416.el5
kernel-PAE-devel-2.6.18-416.el5
kernel-debuginfo-common-2.6.18-416.el5
kernel-debug-debuginfo-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-xen-2.6.18-416.el5
kernel-PAE-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-xen-debuginfo-2.6.18-416.el5
kernel-PAE-debuginfo-2.6.18-416.el5

kernel-headers-2.6.18-416.el5

noarch
kernel-doc-2.6.18-416.el5

x86_64
kernel-debug-debuginfo-2.6.18-416.el5
kernel-debuginfo-common-2.6.18-416.el5
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-headers-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-xen-debuginfo-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-2.6.18-416.el5
kernel-debuginfo-2.6.18-416.el5

178229 - Gentoo Linux GLSA-201610-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5127, CVE-2016-5128, CVE-2016-5129, CVE-2016-5130, CVE-2016-5131, CVE-2016-5132, CVE-2016-5133, CVE-2016-5134, CVE-2016-5135, CVE-2016-5136, CVE-2016-5137, CVE-2016-5138, CVE-2016-5139, CVE-2016-5140, CVE-2016-5141, CVE-2016-5142, CVE-2016-5143, CVE-2016-5144, CVE-2016-5145, CVE-2016-5146, CVE-2016-5147, CVE-2016-5148, CVE-2016-5149, CVE-2016-5150, CVE-2016-5151, CVE-2016-5152, CVE-2016-5153, CVE-2016-5154, CVE-2016-5155, CVE-2016-5156, CVE-2016-5157, CVE-2016-5158, CVE-2016-5159, CVE-2016-5160, CVE-2016-5161, CVE-2016-5162, CVE-2016-5163, CVE-2016-5164, CVE-2016-5165, CVE-2016-5166, CVE-2016-5167, CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175, CVE-2016-5177, CVE-2016-5178, CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

Description

The scan detected that the host is missing the following update:
GLSA-201610-09

Observation

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

https://security.gentoo.org/glsa/201610-09

Affected packages:
www-client/chromium < 54.0.2840.59

185465 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3117-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-7568, CVE-2016-8670

Description

The scan detected that the host is missing the following update:
USN-3117-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003614.html

Ubuntu 12.04

libgd2-xpm_2.0.36~rc1~dfsg-6ubuntu2.3
libgd2-noxpm_2.0.36~rc1~dfsg-6ubuntu2.3

Ubuntu 16.04

libgd3_2.1.1-4ubuntu0.16.04.5

Ubuntu 14.04

libgd3_2.1.0-3ubuntu0.5

Ubuntu 16.10

libgd3_2.2.1-1ubuntu3.2

191323 - Fedora Linux 24 FEDORA-2016-7a3a0f0198 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5180

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7a3a0f0198

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/2016/10/?count=200&page=3

Fedora Core 24

nodejs-4.6.1-6.fc24

20727 - Oracle Database Server Critical Patch Update October 2016

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

Risk Level: Medium

CVE: CVE-2016-3562, CVE-2016-5497, CVE-2016-5498, CVE-2016-5499, CVE-2016-5505, CVE-2016-5516, CVE-2016-5555, CVE-2016-5572

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

20728 - Oracle Database Server Critical Patch Update October 2016

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-3562, CVE-2016-5497, CVE-2016-5498, CVE-2016-5499, CVE-2016-5505, CVE-2016-5516, CVE-2016-5555, CVE-2016-5572

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

20746 - (JSA10763) Juniper Junos Multiple Privilege Escalation Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-4922

Description

Multiple vulnerabilities are present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper Networks hardware routers.

Multiple vulnerabilities are present in some versions of Juniper Junos. The flaws lie in Junos CLI. Successful exploitation could allow an attacker to gain elevated privileges.

88818 - Slackware Linux 14.1, 14.2 SSA:2016-305-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5584, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-7440, CVE-2016-8283

Description

The scan detected that the host is missing the following update:
SSA:2016-305-03

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=2016&m=slackware-security.484350

Slackware 14.1
x86_64

mariadb-5.5.53-x86_64-1

Slackware 14.2
x86_64
mariadb-10.0.28-x86_64-1

i586
mariadb-10.0.28-i586-1

185464 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3118-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6893, CVE-2016-7123

Description

The scan detected that the host is missing the following update:
USN-3118-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003613.html

Ubuntu 12.04

mailman_2.1.14-3ubuntu0.4

Ubuntu 16.04

mailman_2.1.20-1ubuntu0.1

Ubuntu 14.04

mailman_2.1.16-2ubuntu0.2

Ubuntu 16.10

mailman_2.1.22-1ubuntu0.1

178230 - Gentoo Linux GLSA-201611-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6329

Description

The scan detected that the host is missing the following update:
GLSA-201611-02

Observation

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

https://security.gentoo.org/glsa/201611-02

Affected packages:
net-misc/openvpn < 2.3.12

178231 - Gentoo Linux GLSA-201611-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8139, CVE-2014-8140, CVE-2014-8141, CVE-2014-9636

Description

The scan detected that the host is missing the following update:
GLSA-201611-01

Observation

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

https://security.gentoo.org/glsa/201611-01

Affected packages:
app-arch/unzip < 6.0_p20

141317 - Red Hat Enterprise Linux RHSA-2016-2128 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2128

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2128.html

RHEL6_6S
i386
kernel-2.6.32-504.54.1.el6
kernel-headers-2.6.32-504.54.1.el6
kernel-devel-2.6.32-504.54.1.el6
perf-2.6.32-504.54.1.el6
kernel-debuginfo-2.6.32-504.54.1.el6
python-perf-debuginfo-2.6.32-504.54.1.el6
perf-debuginfo-2.6.32-504.54.1.el6
kernel-debuginfo-common-i686-2.6.32-504.54.1.el6
kernel-debug-2.6.32-504.54.1.el6
kernel-debug-devel-2.6.32-504.54.1.el6
kernel-debug-debuginfo-2.6.32-504.54.1.el6

noarch
kernel-doc-2.6.32-504.54.1.el6
kernel-abi-whitelists-2.6.32-504.54.1.el6

kernel-firmware-2.6.32-504.54.1.el6

x86_64
kernel-2.6.32-504.54.1.el6
kernel-headers-2.6.32-504.54.1.el6
kernel-devel-2.6.32-504.54.1.el6
perf-2.6.32-504.54.1.el6
kernel-debuginfo-2.6.32-504.54.1.el6
python-perf-debuginfo-2.6.32-504.54.1.el6
perf-debuginfo-2.6.32-504.54.1.el6
kernel-debuginfo-common-i686-2.6.32-504.54.1.el6
kernel-debug-2.6.32-504.54.1.el6
kernel-debug-devel-2.6.32-504.54.1.el6
kernel-debug-debuginfo-2.6.32-504.54.1.el6
kernel-debuginfo-common-x86_64-2.6.32-504.54.1.el6

178228 - Gentoo Linux GLSA-201610-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4971

Description

The scan detected that the host is missing the following update:
GLSA-201610-11

Observation

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

https://security.gentoo.org/glsa/201610-11

Affected packages:
net-misc/wget < 1.18

88817 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-305-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5407, CVE-2016-7942, CVE-2016-7943, CVE-2016-7944, CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948, CVE-2016-7949, CVE-2016-7950, CVE-2016-7951, CVE-2016-7952, CVE-2016-7953

Description

The scan detected that the host is missing the following update:
SSA:2016-305-02

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=2016&m=slackware-security.3362343

Slackware 14.0
noarch
inputproto-2.3.2-noarch-1
xproto-7.0.29-noarch-1

randrproto-1.5.0-noarch-1

x86_64
libXrandr-1.5.1-x86_64-1
libX11-1.6.4-x86_64-1
libXfixes-5.0.3-x86_64-1
xcb-proto-1.11-x86_64-1
libXrender-0.9.10-x86_64-1
libXext-1.3.3-x86_64-1
xextproto-7.3.0-x86_64-1
libXtst-1.2.3-x86_64-1
libxcb-1.11.1-x86_64-1
libXvMC-1.0.10-x86_64-1
libXi-1.7.8-x86_64-1
libXv-1.0.11-x86_64-1

Slackware 13.37
noarch
inputproto-2.3.2-noarch-1
xproto-7.0.29-noarch-1
randrproto-1.5.0-noarch-1
recordproto-1.14.2-noarch-1

x86_64
libXrandr-1.5.1-x86_64-1
libX11-1.6.4-x86_64-1
libXfixes-5.0.3-x86_64-1
xcb-proto-1.11-x86_64-1
libXrender-0.9.10-x86_64-1
libXext-1.3.3-x86_64-1
xextproto-7.3.0-x86_64-1
libXtst-1.2.3-x86_64-1
libxcb-1.11.1-x86_64-1
libXvMC-1.0.10-x86_64-1
libXi-1.7.8-x86_64-1
libXv-1.0.11-x86_64-1

Slackware 14.1
noarch
inputproto-2.3.2-noarch-1
xproto-7.0.29-noarch-1
randrproto-1.5.0-noarch-1

x86_64
libXrandr-1.5.1-x86_64-1
libX11-1.6.4-x86_64-1
libXfixes-5.0.3-x86_64-1
xcb-proto-1.11-x86_64-1
libXrender-0.9.10-x86_64-1
libXext-1.3.3-x86_64-1
xextproto-7.3.0-x86_64-1
libXtst-1.2.3-x86_64-1
libxcb-1.11.1-x86_64-1
libXvMC-1.0.10-x86_64-1
libXi-1.7.8-x86_64-1
libXv-1.0.11-x86_64-1

Slackware 13.1
noarch
inputproto-2.3.2-noarch-1

xproto-7.0.29-noarch-1
randrproto-1.5.0-noarch-1
recordproto-1.14.2-noarch-1

x86_64
xextproto-7.3.0-x86_64-1
libXi-1.7.8-x86_64-1
libX11-1.6.4-x86_64-1
libXtst-1.2.3-x86_64-1
libXrandr-1.5.1-x86_64-1
libXrender-0.9.10-x86_64-1
libxcb-1.11.1-x86_64-1
xcb-proto-1.11-x86_64-1
libXfixes-5.0.3-x86_64-1
libXvMC-1.0.10-x86_64-1
libXext-1.3.3-x86_64-1
libXv-1.0.11-x86_64-1
fixesproto-5.0-x86_64-1

Slackware 14.2
x86_64
libXrandr-1.5.1-x86_64-1
libX11-1.6.4-x86_64-1
libXfixes-5.0.3-x86_64-1
libXrender-0.9.10-x86_64-1
libXvMC-1.0.10-x86_64-1
libXtst-1.2.3-x86_64-1
libXi-1.7.8-x86_64-1
libXv-1.0.11-x86_64-1

i586
libXfixes-5.0.3-i586-1
libXrender-0.9.10-i586-1
libXi-1.7.8-i586-1
libXrandr-1.5.1-i586-1
libX11-1.6.4-i586-1
libXtst-1.2.3-i586-1
libXvMC-1.0.10-i586-1
libXv-1.0.11-i586-1

Slackware 13.0
noarch
inputproto-2.3.2-noarch-1
xproto-7.0.29-noarch-1
randrproto-1.5.0-noarch-1
recordproto-1.14.2-noarch-1

x86_64
xextproto-7.3.0-x86_64-1
libXi-1.7.8-x86_64-1
libX11-1.6.4-x86_64-1
libXtst-1.2.3-x86_64-1
libXrandr-1.5.1-x86_64-1
libXrender-0.9.10-x86_64-1
libxcb-1.11.1-x86_64-1
xcb-proto-1.11-x86_64-1
libXfixes-5.0.3-x86_64-1
libXvMC-1.0.10-x86_64-1
libXext-1.3.3-x86_64-1
libXv-1.0.11-x86_64-1

fixesproto-5.0-x86_64-1

88819 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-305-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
SSA:2016-305-01

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=2016&m=slackware-security.1350971

Slackware 14.0
x86_64
kernel-modules-3.2.83-x86_64-1
kernel-generic-3.2.83-x86_64-1
kernel-huge-3.2.83-x86_64-1

noarch
kernel-source-3.2.83-noarch-1

Slackware 14.2
i586
kernel-modules-4.4.29-i586-1
kernel-generic-4.4.29-i586-1
kernel-huge-4.4.29-i586-1

i686
kernel-generic-smp-4.4.29_smp-i686-1
kernel-huge-smp-4.4.29_smp-i686-1
kernel-modules-smp-4.4.29_smp-i686-1

noarch
kernel-source-4.4.29_smp-noarch-1
kernel-source-4.4.29-noarch-1

x86_64
kernel-huge-4.4.29-x86_64-1
kernel-modules-4.4.29-x86_64-1
kernel-generic-4.4.29-x86_64-1

Slackware 14.1
i686
kernel-huge-smp-3.10.104_smp-i686-1
kernel-generic-smp-3.10.104_smp-i686-1
kernel-modules-smp-3.10.104_smp-i686-1

noarch
kernel-source-3.10.104_smp-noarch-1
kernel-source-3.10.104-noarch-1

x86_64

kernel-huge-3.10.104-x86_64-1
kernel-modules-3.10.104-x86_64-1
kernel-generic-3.10.104-x86_64-1

88820 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-305-04 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:2016-305-04

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=2016&m=slackware-security.413956

Slackware 14.0
x86_64
php-5.6.27-x86_64-1

Slackware 14.2
x86_64
php-5.6.27-x86_64-1

i586
php-5.6.27-i586-1

Slackware 14.1
x86_64
php-5.6.27-x86_64-1

130617 - Debian Linux 8.0 DSA-3702-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6321

Description

The scan detected that the host is missing the following update:
DSA-3702-1

Observation

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

http://www.debian.org/security/2016/dsa-3702

Debian 8.0
all
tar_1.27.1-2+deb8u1

130618 - Debian Linux 8.0 DSA-3703-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
DSA-3703-1

Observation

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

http://www.debian.org/security/2016/dsa-3703

Debian 8.0
all
bind9_1:9.9.5.dfsg-9+deb8u8

141315 - Red Hat Enterprise Linux RHSA-2016-2135 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-2016-2135

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2135.html

RHEL6_6S
i386
redhat-release-server-6Server-6.6.0.5.el6_6

x86_64
redhat-release-server-6Server-6.6.0.5.el6_6

182156 - FreeBSD django Multiple Vulnerabilities (cb116651-79db-4c09-93a2-c38f9df46724)

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

Risk Level: Low

CVE: CVE-2016-9013, CVE-2016-9014

Description

The scan detected that the host is missing the following update:
django -- multiple vulnerabilities (cb116651-79db-4c09-93a2-c38f9df46724)

Observation

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

http://www.vuxml.org/freebsd/cb116651-79db-4c09-93a2-c38f9df46724.html

Affected packages:
py27-django < 1.8.16
py33-django < 1.8.16
py34-django < 1.8.16
py35-django < 1.8.16
py27-django18 < 1.9.11
py33-django18 < 1.9.11
py34-django18 < 1.9.11
py35-django18 < 1.9.11
py27-django19 < 1.10.3
py33-django19 < 1.10.3
py34-django19 < 1.10.3
py35-django19 < 1.10.3

182157 - FreeBSD chromium Multiple Vulnerabilities (9118961b-9fa5-11e6-a265-3065ec8fd3ec)

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

Risk Level: Low

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (9118961b-9fa5-11e6-a265-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/9118961b-9fa5-11e6-a265-3065ec8fd3ec.html

Affected packages:
chromium < 54.0.2840.59
chromium-npapi < 54.0.2840.59
chromium-pulse < 54.0.2840.59

182158 - FreeBSD chromium Multiple Vulnerabilities (9c135c7e-9fa4-11e6-a265-3065ec8fd3ec)

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

Risk Level: Low

CVE: CVE-2016-5177, CVE-2016-5178

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (9c135c7e-9fa4-11e6-a265-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/9c135c7e-9fa4-11e6-a265-3065ec8fd3ec.html

Affected packages:
chromium < 53.0.2785.143
chromium-npapi < 53.0.2785.143
chromium-pulse < 53.0.2785.143

182159 - FreeBSD memcached Multiple Vulnerabilities (f4bf713f-6ac7-4b76-8980-47bf90c5419f)

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

Risk Level: Low

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

Description

The scan detected that the host is missing the following update:
memcached -- multiple vulnerabilities (f4bf713f-6ac7-4b76-8980-47bf90c5419f)

Observation

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

http://www.vuxml.org/freebsd/f4bf713f-6ac7-4b76-8980-47bf90c5419f.html

Affected packages:
memcached < 1.4.33

182160 - FreeBSD FreeBSD OpenSSH Remote Denial Of Service Vulnerability (6a2cfcdc-9dea-11e6-a298-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-8858

Description

The scan detected that the host is missing the following update:
FreeBSD -- OpenSSH Remote Denial of Service vulnerability (6a2cfcdc-9dea-11e6-a298-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/6a2cfcdc-9dea-11e6-a298-14dae9d210b8.html

Affected packages:
openssh-portable < 7.3p1_1
11.0 <= FreeBSD < 11.0_3
10.3 <= FreeBSD < 10.3_12

182161 - FreeBSD sudo Potential Bypass Of Sudo_noexec.so Via Wordexp () (2e4fbc9a-9d23-11e6-a298-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-7076

Description

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

sudo -- Potential bypass of sudo_noexec.so via wordexp() (2e4fbc9a-9d23-11e6-a298-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/2e4fbc9a-9d23-11e6-a298-14dae9d210b8.html

Affected packages:
1.6.8 <= sudo < 1.8.18p1

182162 - FreeBSD BIND Remote Denial Of Service Vulnerability (0b8d01a4-a0d2-11e6-9ca2-d050996490d0)

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

Risk Level: Low

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
BIND -- Remote Denial of Service vulnerability (0b8d01a4-a0d2-11e6-9ca2-d050996490d0)

Observation

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

http://www.vuxml.org/freebsd/0b8d01a4-a0d2-11e6-9ca2-d050996490d0.html

Affected packages:
bind99 < 9.9.9P4
bind910 < 9.10.4P4
bind911 < 9.11.0P1
bind9-devel <= 9.12.0.a.2016.10.21
9.3 <= FreeBSD < 9.3_50

182163 - FreeBSD MySQL Multiple Vulnerabilities (9bc14850-a070-11e6-a881-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-5584, CVE-2016-7440

Description

The scan detected that the host is missing the following update:
MySQL -- multiple vulnerabilities (9bc14850-a070-11e6-a881-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/9bc14850-a070-11e6-a881-b499baebfeaf.html

Affected packages:
mariadb55-server < 5.5.53
mysql55-server < 5.5.53
mysql56-server < 5.6.34
mysql57-server < 5.7.15

182164 - FreeBSD cURL Multiple Vulnerabilities (765feb7d-a0d1-11e6-a881-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625

Description

The scan detected that the host is missing the following update:
cURL -- multiple vulnerabilities (765feb7d-a0d1-11e6-a881-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/765feb7d-a0d1-11e6-a881-b499baebfeaf.html

Affected packages:
7.1 <= curl < 7.51.0

182165 - FreeBSD FreeBSD OpenSSL Remote DoS Vulnerability (0fcd3af0-a0fe-11e6-b1cf-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-8610

Description

The scan detected that the host is missing the following update:
FreeBSD -- OpenSSL Remote DoS vulnerability (0fcd3af0-a0fe-11e6-b1cf-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/0fcd3af0-a0fe-11e6-b1cf-14dae9d210b8.html

Affected packages:
10.3 <= FreeBSD < 10.3_12
10.2 <= FreeBSD < 10.2_25
10.1 <= FreeBSD < 10.1_42
9.3 <= FreeBSD < 9.3_50
openssl < 1.0.2j,1
openssl-devel < 1.1.0b

185466 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3115-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9013, CVE-2016-9014

Description

The scan detected that the host is missing the following update:
USN-3115-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003611.html

Ubuntu 12.04

python-django_1.3.1-4ubuntu1.22

Ubuntu 16.04

python3-django_1.8.7-1ubuntu5.4
python-django_1.8.7-1ubuntu5.4

Ubuntu 14.04

python-django_1.6.1-2ubuntu0.16

Ubuntu 16.10

python-django_1.8.7-1ubuntu8.1
python3-django_1.8.7-1ubuntu8.1

185468 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3119-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
USN-3119-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003615.html

Ubuntu 12.04

bind9_9.8.1.dfsg.P1-4ubuntu0.19

Ubuntu 16.04

bind9_9.10.3.dfsg.P4-8ubuntu1.2

Ubuntu 14.04

bind9_9.9.5.dfsg-3ubuntu0.10

Ubuntu 16.10

bind9_9.10.3.dfsg.P4-10.1ubuntu1.1

191312 - Fedora Linux 23 FEDORA-2016-0e7694c456 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7944

Description

The scan detected that the host is missing the following update:
FEDORA-2016-0e7694c456

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/2016/11/?count=200&page=1

Fedora Core 23

libXfixes-5.0.3-1.fc23

191313 - Fedora Linux 25 FEDORA-2016-e56ed6f472 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8860

Description

The scan detected that the host is missing the following update:
FEDORA-2016-e56ed6f472

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/2016/10/?count=200&page=1

Fedora Core 25

tor-0.2.8.9-1.fc25

191314 - Fedora Linux 23 FEDORA-2016-d286ffb801 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7953

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d286ffb801

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/2016/11/?count=200&page=1

Fedora Core 23

libXvMC-1.0.10-1.fc23

191315 - Fedora Linux 23 FEDORA-2016-49d560da23 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7949, CVE-2016-7950

Description

The scan detected that the host is missing the following update:
FEDORA-2016-49d560da23

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/2016/11/?count=200&page=1

Fedora Core 23

libXrender-0.9.10-1.fc23

191316 - Fedora Linux 23 FEDORA-2016-3b6393acdd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8860

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3b6393acdd

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/2016/11/?count=200&page=1

Fedora Core 23

tor-0.2.8.9-1.fc23

191317 - Fedora Linux 23 FEDORA-2016-3b41a9eaa8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5407

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3b41a9eaa8

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/2016/11/?count=200&page=1

Fedora Core 23

libXv-1.0.11-1.fc23

191318 - Fedora Linux 24 FEDORA-2016-59316cf667 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8860

Description

The scan detected that the host is missing the following update:
FEDORA-2016-59316cf667

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/2016/11/?count=200&page=1

Fedora Core 24

tor-0.2.8.9-1.fc24

191319 - Fedora Linux 25 FEDORA-2016-92c112a380 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

Description

The scan detected that the host is missing the following update:
FEDORA-2016-92c112a380

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/2016/10/?count=200&page=1

Fedora Core 25

kdepimlibs-4.14.10-15.fc25

191321 - Fedora Linux 23 FEDORA-2016-8e4e733bef 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-2016-8e4e733bef

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/2016/11/?count=200&page=1

Fedora Core 23

systemd-222-17.fc23

191322 - Fedora Linux 23 FEDORA-2016-95407a836f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7969, CVE-2016-7970, CVE-2016-7971, CVE-2016-7972

Description

The scan detected that the host is missing the following update:
FEDORA-2016-95407a836f

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/2016/11/?count=200&page=1

Fedora Core 23

libass-0.13.4-1.fc23

191324 - Fedora Linux 24 FEDORA-2016-1b042a79bd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1b042a79bd

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/2016/10/?count=200&page=2
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1

Fedora Core 24

kf5-mailimporter-16.08.2-1.fc24
kdepim-16.08.2-1.fc24
kf5-kontactinterface-16.08.2-1.fc24
kf5-syndication-16.08.2-1.fc24
kdepim-apps-libs-16.08.2-1.fc24
kf5-kcalendarutils-16.08.2-1.fc24
kf5-grantleetheme-16.08.2-1.fc24
kf5-kcalendarcore-16.08.2-1.fc24
kf5-kimap-16.08.2-1.fc24
kf5-akonadi-notes-16.08.2-1.fc24
kf5-kcontacts-16.08.2-1.fc24
kf5-akonadi-mime-16.08.2-1.fc24
kf5-kpimtextedit-16.08.2-1.fc24
kf5-kdgantt2-16.08.2-1.fc24
kf5-kidentitymanagement-16.08.2-1.fc24
kf5-kmailtransport-16.08.2-1.fc24
kf5-akonadi-search-16.08.2-1.fc24
kf5-mailcommon-16.08.2-1.fc24
kf5-messagelib-16.08.2-1.fc24
kf5-akonadi-contacts-16.08.2-1.fc24
kf5-kmbox-16.08.2-1.fc24
kf5-kholidays-16.08.2-1.fc24
kf5-pimcommon-16.08.2-1.fc24
kdepim-runtime-16.08.2-1.fc24
kf5-akonadi-server-16.08.2-1.fc24
kf5-libkdepim-16.08.2-1.fc24
kf5-eventviews-16.08.2-1.fc24
kf5-incidenceeditor-16.08.2-1.fc24
kf5-kmime-16.08.2-1.fc24
kf5-kalarmcal-16.08.2-1.fc24
kf5-gpgmepp-16.08.2-1.fc24
kf5-ktnef-16.08.2-1.fc24
kf5-libkleo-16.08.2-1.fc24
kf5-libgravatar-16.08.2-1.fc24
kdepim-addons-16.08.2-1.fc24
kf5-calendarsupport-16.08.2-1.fc24
kf5-kldap-16.08.2-1.fc24
kf5-kblog-16.08.2-1.fc24
kf5-akonadi-calendar-16.08.2-1.fc24
kleopatra-16.08.2-1.fc24
kf5-libksieve-16.08.2-1.fc24

191325 - Fedora Linux 23 FEDORA-2016-b26b497381 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7951, CVE-2016-7952

Description

The scan detected that the host is missing the following update:
FEDORA-2016-b26b497381

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/2016/11/?count=200&page=1

Fedora Core 23

libXtst-1.2.3-1.fc23

191326 - Fedora Linux 23 FEDORA-2016-d045c2c7b3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7947, CVE-2016-7948

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d045c2c7b3

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/2016/11/?count=200&page=1

Fedora Core 23

libXrandr-1.5.1-1.fc23

191320 - Fedora Linux 23 FEDORA-2016-70b5173c05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8946, CVE-2016-6224

Description

The scan detected that the host is missing the following update:
FEDORA-2016-70b5173c05

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/2016/11/?count=200&page=1

Fedora Core 23

ecryptfs-utils-111-1.fc23

185467 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3116-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0245

Description

The scan detected that the host is missing the following update:
USN-3116-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003612.html

Ubuntu 12.04

dbus_1.4.18-1ubuntu1.8
libdbus-1-3_1.4.18-1ubuntu1.8

Ubuntu 16.04

dbus_1.10.6-1ubuntu3.1
libdbus-1-3_1.10.6-1ubuntu3.1

Ubuntu 14.04

dbus_1.6.18-0ubuntu4.4
libdbus-1-3_1.6.18-0ubuntu4.4

Ubuntu 16.10

libdbus-1-3_1.10.10-1ubuntu1.1
dbus_1.10.10-1ubuntu1.1

ENHANCED CHECKS

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

20016 - (MS16-055) Security Update for Microsoft Graphics Component (3156754)

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

Risk Level: High

CVE: CVE-2016-0168, CVE-2016-0169, CVE-2016-0170, CVE-2016-0184, CVE-2016-0195

Update Details

FASLScript is updated

20020 - (MS16-055) Microsoft Windows Graphics Direct3D Remote Code Execution (3156754)

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

Risk Level: High

CVE: CVE-2016-0184

Update Details

FASLScript is updated

130614 - Debian Linux 8.0 DSA-3698-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9137

Update Details

CVE is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.