2017-APR-27
FSL version 7.5.916

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

21646 - (HPSBMU03691) HPE System Management Homepage Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2009-5028, CVE-2011-4345, CVE-2014-0050, CVE-2014-4877, CVE-2015-5125, 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-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5548, CVE-2015-5549, 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-2015-5565, CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-6420, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6682, CVE-2015-7547, CVE-2015-8044, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8434, CVE-2015-8435, CVE-2015-8441, CVE-2015-8442, 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-2015-8460, CVE-2015-8634, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2016-4537, CVE-2016-4538, CVE-2016-5385, CVE-2016-8517

Description

Multiple vulnerabilities are present in some versions of HPE System Management Homepage.

Observation

HPE System Management Homepage is a web-based interface that consolidates and simplifies the management of individual ProLiant and Integrity servers.

Multiple vulnerabilities are present in some versions of HPE System Management Homepage. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code on the target system.

21647 - (HPSBMU03691) HP Systems Insight Manager Multiple Vulnerabilities

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

Risk Level: High

CVE: 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-2015-8459, 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-2016-0702, CVE-2016-0705, CVE-2016-0777, CVE-2016-0778, CVE-2016-0797, CVE-2016-0799, CVE-2016-1521, CVE-2016-1907, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2183, CVE-2016-2842, CVE-2016-3739, CVE-2016-4070, CVE-2016-4071, CVE-

2016-4072, CVE-2016-4342, CVE-2016-4343, CVE-2016-4393, CVE-2016-4394, CVE-2016-4395, CVE-2016-4396, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-5385, CVE-2016-5387, CVE-2016-5388, CVE-2016-8513, CVE-2016-8514, CVE-2016-8515, CVE-2016-8516, CVE-2016-8517, CVE-2016-8518, CVE-2017-5787

Description

Multiple vulnerabilities are present in some versions of HP Systems Insight Manager.

Observation

HP Systems Insight Manager is a hardware management solution.

Multiple vulnerabilities are present in some versions of HP Systems Insight Manager. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code on the target system.

21648 - (HPSBMU03691) HPE Version Control Repository Manager Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2009-5028, CVE-2011-4345, CVE-2014-0050, CVE-2014-4877, CVE-2015-5125, 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, CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6420, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6679, CVE-2015-6682, CVE-2015-7547, CVE-2015-8044, 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

Description

Multiple vulnerabilities are present in some versions of HPE Version Control Repository Manager.

Observation

HPE Version Control Repository Manager lets customers to manage HP software stored in their repositories.

Multiple vulnerabilities are present in some versions of HPE Version Control Repository Manager. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code on the target system.

21668 - (CTX222657) Citrix NetScaler Gateway Heap Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-7219

Description

A buffer overflow vulnerability is present in some versions of Citrix NetScaler Gateway.

Observation

Citrix NetScaler Gateway is a secure network access gateway.

A buffer overflow vulnerability is present in some versions of Citrix NetScaler Gateway. The flaw is due to unspecified vectors. Successful exploitation could allow an attacker to remotely execute arbitrary code.

132357 - Oracle VM OVMSA-2017-0061 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10229, CVE-2016-7910

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0061

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000677.html

OVM3.2
x86_64
kernel-uek-2.6.39-400.294.7.el5uek
kernel-uek-firmware-2.6.39-400.294.7.el5uek

141544 - Red Hat Enterprise Linux RHSA-2017-0934 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3061, CVE-2017-3062, CVE-2017-3063, CVE-2017-3064

Description

The scan detected that the host is missing the following update:
RHSA-2017-0934

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00018.html

RHEL6D
x86_64
flash-plugin-25.0.0.148-1.el6_9

i386
flash-plugin-25.0.0.148-1.el6_9

RHEL6S
x86_64
flash-plugin-25.0.0.148-1.el6_9

i386
flash-plugin-25.0.0.148-1.el6_9

RHEL6WS
x86_64
flash-plugin-25.0.0.148-1.el6_9

i386
flash-plugin-25.0.0.148-1.el6_9

145304 - SuSE SLED 12 SP1 SUSE-SU-2017:0990-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3061, CVE-2017-3062, CVE-2017-3063, CVE-2017-3064

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0990-1

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-April/002794.html

SuSE SLED 12 SP1
x86_64
flash-player-gnome-25.0.0.148-165.1
flash-player-25.0.0.148-165.1

163331 - Oracle Enterprise Linux ELSA-2017-3538 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10229, CVE-2016-7910

Description

The scan detected that the host is missing the following update:
ELSA-2017-3538

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006857.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006856.html

OEL5
x86_64
kernel-uek-debug-devel-2.6.39-400.294.7.el5uek
kernel-uek-devel-2.6.39-400.294.7.el5uek
kernel-uek-2.6.39-400.294.7.el5uek
kernel-uek-doc-2.6.39-400.294.7.el5uek
kernel-uek-debug-2.6.39-400.294.7.el5uek
kernel-uek-firmware-2.6.39-400.294.7.el5uek

i386
kernel-uek-debug-devel-2.6.39-400.294.7.el5uek

kernel-uek-devel-2.6.39-400.294.7.el5uek
kernel-uek-2.6.39-400.294.7.el5uek
kernel-uek-doc-2.6.39-400.294.7.el5uek
kernel-uek-debug-2.6.39-400.294.7.el5uek
kernel-uek-firmware-2.6.39-400.294.7.el5uek

OEL6
x86_64
kernel-uek-devel-2.6.39-400.294.7.el6uek
kernel-uek-debug-2.6.39-400.294.7.el6uek
kernel-uek-firmware-2.6.39-400.294.7.el6uek
kernel-uek-debug-devel-2.6.39-400.294.7.el6uek
kernel-uek-2.6.39-400.294.7.el6uek
kernel-uek-doc-2.6.39-400.294.7.el6uek

i386
kernel-uek-devel-2.6.39-400.294.7.el6uek
kernel-uek-debug-2.6.39-400.294.7.el6uek
kernel-uek-firmware-2.6.39-400.294.7.el6uek
kernel-uek-debug-devel-2.6.39-400.294.7.el6uek
kernel-uek-2.6.39-400.294.7.el6uek
kernel-uek-doc-2.6.39-400.294.7.el6uek

21667 - Wecon Technologies LEVI Studio HMI Editor Two Buffer Overflow Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-6035, CVE-2017-6037

Description

Two buffer overflow vulnerabilities are present in some versions of Wecon Levi Studio HMI Editor.

Observation

Wecon Levi Studio is an HMI programming software.

Two buffer overflow vulnerabilities are present in some versions of Wecon Levi Studio. The flaws occur due to stack based buffer overflow and heap based buffer overflow. Successful exploitation could allow an attacker to execute arbitrary code by tricking the system to run a maliciously crafted project file.

21671 - (APSB17-12) Vulnerabilities In Adobe Photoshop CC

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

Risk Level: High

CVE: CVE-2017-3004, CVE-2017-3005

Description

Multiple vulnerabilities are present in some versions of Adobe Photoshop CC.

Observation

Adobe Photoshop CC is a product for media editing and management.

Multiple vulnerabilities are present in some versions of Adobe Photoshop CC. The flaws lie in several components. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

21672 - (APSB17-12) Vulnerabilities In Adobe Photoshop CC

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-3004, CVE-2017-3005

Description

Multiple vulnerabilities are present in some versions of Adobe Photoshop CC.

Observation

Adobe Photoshop CC is a product for media editing and management.

Multiple vulnerabilities are present in some versions of Adobe Photoshop CC. The flaws lie in several components. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

21686 - (VMSA-2017-0008) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4908, CVE-2017-4909, CVE-2017-4910, CVE-2017-4911, CVE-2017-4912, CVE-2017-4913

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow a remote attacker to execute code or cause a denial of service condition.

132356 - Oracle VM OVMSA-2017-0062 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10208, CVE-2016-7910, CVE-2017-2583, CVE-2017-5986, CVE-2017-6214, CVE-2017-6347, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0062

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000678.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-61.1.34.el6uek
kernel-uek-4.1.12-61.1.34.el6uek

132358 - Oracle VM OVMSA-2017-0060 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0060

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000679.html

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.17.5.el6uek
kernel-uek-3.8.13-118.17.5.el6uek

160237 - CentOS 6 CESA-2017-0892 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
CESA-2017-0892

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-April/022358.html

CentOS 6
i686
kernel-headers-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6

noarch
kernel-firmware-2.6.32-696.1.1.el6
kernel-doc-2.6.32-696.1.1.el6
kernel-abi-whitelists-2.6.32-696.1.1.el6

x86_64
kernel-headers-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6

perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6

163325 - Oracle Enterprise Linux ELSA-2017-3539 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10208, CVE-2016-7910, CVE-2017-2583, CVE-2017-5986, CVE-2017-6214, CVE-2017-6347, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
ELSA-2017-3539

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006859.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006860.html

OEL7
x86_64
kernel-uek-devel-4.1.12-61.1.34.el7uek
kernel-uek-doc-4.1.12-61.1.34.el7uek
kernel-uek-debug-devel-4.1.12-61.1.34.el7uek
kernel-uek-firmware-4.1.12-61.1.34.el7uek
kernel-uek-debug-4.1.12-61.1.34.el7uek
kernel-uek-4.1.12-61.1.34.el7uek
dtrace-modules-4.1.12-61.1.34.el7uek-0.5.3-2.el7

OEL6
x86_64
kernel-uek-firmware-4.1.12-61.1.34.el6uek
dtrace-modules-4.1.12-61.1.34.el6uek-0.5.3-2.el6
kernel-uek-devel-4.1.12-61.1.34.el6uek
kernel-uek-debug-devel-4.1.12-61.1.34.el6uek
kernel-uek-doc-4.1.12-61.1.34.el6uek
kernel-uek-4.1.12-61.1.34.el6uek
kernel-uek-debug-4.1.12-61.1.34.el6uek

163326 - Oracle Enterprise Linux ELSA-2017-3537 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910

Description

The scan detected that the host is missing the following update:
ELSA-2017-3537

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006861.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006862.html

OEL7
x86_64
kernel-uek-firmware-3.8.13-118.17.5.el7uek
kernel-uek-3.8.13-118.17.5.el7uek
dtrace-modules-3.8.13-118.17.5.el7uek-0.4.5-3.el7
kernel-uek-debug-3.8.13-118.17.5.el7uek
kernel-uek-doc-3.8.13-118.17.5.el7uek
kernel-uek-devel-3.8.13-118.17.5.el7uek
kernel-uek-debug-devel-3.8.13-118.17.5.el7uek

OEL6
x86_64
dtrace-modules-3.8.13-118.17.5.el6uek-0.4.5-3.el6
kernel-uek-firmware-3.8.13-118.17.5.el6uek
kernel-uek-doc-3.8.13-118.17.5.el6uek
kernel-uek-devel-3.8.13-118.17.5.el6uek
kernel-uek-debug-devel-3.8.13-118.17.5.el6uek
kernel-uek-3.8.13-118.17.5.el6uek
kernel-uek-debug-3.8.13-118.17.5.el6uek

191945 - Fedora Linux 24 FEDORA-2017-e2a3e6fa12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7413, CVE-2017-7414

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e2a3e6fa12

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/2017/4/?count=200&page=3

Fedora Core 24

php-horde-Horde-Crypt-2.7.6-1.fc24

191960 - Fedora Linux 26 FEDORA-2017-36eb9502b0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7572

Description

The scan detected that the host is missing the following update:
FEDORA-2017-36eb9502b0

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/2017/4/?count=200&page=1

Fedora Core 26

backintime-1.1.20-1.fc26

191971 - Fedora Linux 25 FEDORA-2017-ed4c9b605b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7413, CVE-2017-7414

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ed4c9b605b

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/2017/4/?count=200&page=3

Fedora Core 25

php-horde-Horde-Crypt-2.7.6-1.fc25

21666 - Cisco ASA Clientless SSL VPN CIFS Heap Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-3807

Description

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA).

Observation

Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA). The flaw lies in the Clientless SSL VPN functionality. Successful exploitation could allow an attacker to execute remote code or to cause a denial of service.

21642 - (HT207688) Apple iOS Vulnerability Prior To 10.3.1

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2017-6975

Description

A vulnerability is present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

A vulnerability is present in some versions of Apple iOS. The flaw is related with the Wi-Fi functionality. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

21649 - Cisco AnyConnect Secure Mobility Client for Windows SBL Privileges Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2017-3813

Description

A privilege escalation vulnerability is present in some versions of Cisco AnyConnect Secure Mobility Client.

Observation

Cisco AnyConnect Secure Mobility Client is a VPN client software.

A privilege escalation vulnerability is present in some versions of Cisco AnyConnect Secure Mobility Client. The flaw lies in the Start Before Logon (SBL) module. Successful exploitation could allow an attacker to use Internet Explorer with the privileges of the SYSTEM user.

21661 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410, CVE-2017-5411, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5416, CVE-2017-5418, CVE-2017-5419, CVE-2017-5421, CVE-2017-5422, CVE-2017-5425, CVE-2017-5426

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

21662 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410, CVE-2017-5411, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5416, CVE-2017-5418, CVE-2017-5419, CVE-2017-5421, CVE-2017-5422, CVE-2017-5425, CVE-2017-5426

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful

exploitation could allow an attacker to bypass security access restrictions, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

21664 - Novell eDirectory Multiple Vulnerabilities Prior To 8.8 SP8 Patch 10

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6303, CVE-2016-6306

Description

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory.

Observation

Novell (NetIQ) eDirectory is an X.500 compatible directory service software for centrally managing access to network resources.

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory. The flaws lie in multiple components. Successful exploitation could allow a malicious user to cause a denial-of-service, an information disclosure or other unspecified impact.

21683 - Apache Tomcat Multiple Vulnerabilities Prior To 9.0.0.M19

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

Risk Level: High

CVE: CVE-2017-5647, CVE-2017-5650, CVE-2017-5651

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial of service condition.

21684 - Google Chrome Multiple Vulnerabilities Prior To 58.0.3029.81

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

Risk Level: High

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass certain security restrictions, retrieve sensitive data, conduct spoofing attacks, cause a denial of service, or execute arbitrary code.

21685 - Google Chrome Multiple Vulnerabilities Prior To 58.0.3029.81

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass certain security restrictions, retrieve sensitive data, conduct spoofing attacks, cause a denial of service, or execute arbitrary code.

21687 - Oracle Solaris 10 Common Desktop Environment Local Privilege Escalation Vulneravility

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

Risk Level: High

CVE: CVE-2017-3622

Description

A privilege escalation vulnerability is present in some version of Oracle Solaris.

Observation

Oracle Solaris is a Unix-like operation system.

A privilege escalation vulnerability is present in some version of Oracle Solaris. The flaw lies in Common Desktop Environment (CDE). Successful exploitation could allow a local attacker to fully compromise the system.

21694 - Mozilla Firefox Multiple Vulnerabilities Prior To 53

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2016-6354, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5450, CVE-2017-5451, CVE-2017-5452, CVE-2017-5453, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5458, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5463, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information or cause a denial of service condition or execute arbitrary code.

21695 - Mozilla Firefox Multiple Vulnerabilities Prior To 53

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2016-6354, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5450, CVE-2017-5451, CVE-2017-5452, CVE-2017-5453, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5458, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5463, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information or cause a denial of service condition or execute arbitrary code.

141539 - Red Hat Enterprise Linux RHSA-2017-0933 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
RHSA-2017-0933

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00013.html

RHEL7D
x86_64
kernel-debug-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.el7
perf-debuginfo-3.10.0-514.16.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.el7
kernel-tools-libs-3.10.0-514.16.1.el7
kernel-debug-debuginfo-3.10.0-514.16.1.el7
kernel-debug-devel-3.10.0-514.16.1.el7
kernel-tools-debuginfo-3.10.0-514.16.1.el7
kernel-debuginfo-3.10.0-514.16.1.el7
python-perf-3.10.0-514.16.1.el7
kernel-devel-3.10.0-514.16.1.el7
kernel-tools-3.10.0-514.16.1.el7
kernel-debuginfo-common-x86_64-3.10.0-514.16.1.el7
perf-3.10.0-514.16.1.el7
python-perf-debuginfo-3.10.0-514.16.1.el7
kernel-3.10.0-514.16.1.el7

noarch
kernel-abi-whitelists-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.el7

x86_64
kernel-debug-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.el7
perf-debuginfo-3.10.0-514.16.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.el7
kernel-tools-libs-3.10.0-514.16.1.el7
kernel-debug-debuginfo-3.10.0-514.16.1.el7
kernel-debug-devel-3.10.0-514.16.1.el7
kernel-tools-debuginfo-3.10.0-514.16.1.el7
kernel-debuginfo-3.10.0-514.16.1.el7
python-perf-3.10.0-514.16.1.el7
kernel-devel-3.10.0-514.16.1.el7
kernel-tools-3.10.0-514.16.1.el7
kernel-debuginfo-common-x86_64-3.10.0-514.16.1.el7
perf-3.10.0-514.16.1.el7
python-perf-debuginfo-3.10.0-514.16.1.el7
kernel-3.10.0-514.16.1.el7

RHEL7WS
x86_64
kernel-debug-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.el7
perf-debuginfo-3.10.0-514.16.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.el7
kernel-tools-libs-3.10.0-514.16.1.el7
kernel-debug-debuginfo-3.10.0-514.16.1.el7
kernel-debug-devel-3.10.0-514.16.1.el7
kernel-tools-debuginfo-3.10.0-514.16.1.el7
kernel-debuginfo-3.10.0-514.16.1.el7
python-perf-3.10.0-514.16.1.el7
kernel-devel-3.10.0-514.16.1.el7
kernel-tools-3.10.0-514.16.1.el7
kernel-debuginfo-common-x86_64-3.10.0-514.16.1.el7
perf-3.10.0-514.16.1.el7
python-perf-debuginfo-3.10.0-514.16.1.el7
kernel-3.10.0-514.16.1.el7

noarch
kernel-abi-whitelists-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.el7

141540 - Red Hat Enterprise Linux RHSA-2017-0987 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9603

Description

The scan detected that the host is missing the following update:
RHSA-2017-0987

Observation

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

For more information see:

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00030.html

RHEL7D
x86_64
qemu-kvm-debuginfo-1.5.3-126.el7_3.6
qemu-kvm-1.5.3-126.el7_3.6
qemu-kvm-tools-1.5.3-126.el7_3.6
qemu-kvm-common-1.5.3-126.el7_3.6
qemu-img-1.5.3-126.el7_3.6

RHEL7S
x86_64
qemu-kvm-debuginfo-1.5.3-126.el7_3.6
qemu-kvm-1.5.3-126.el7_3.6
qemu-kvm-tools-1.5.3-126.el7_3.6
qemu-kvm-common-1.5.3-126.el7_3.6
qemu-img-1.5.3-126.el7_3.6

RHEL7WS
x86_64
qemu-kvm-debuginfo-1.5.3-126.el7_3.6
qemu-kvm-1.5.3-126.el7_3.6
qemu-kvm-tools-1.5.3-126.el7_3.6
qemu-kvm-common-1.5.3-126.el7_3.6
qemu-img-1.5.3-126.el7_3.6

141542 - Red Hat Enterprise Linux RHSA-2017-0986 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
RHSA-2017-0986

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00029.html

RHEL6_4S
x86_64
kernel-debuginfo-common-x86_64-2.6.32-358.78.1.el6
kernel-devel-2.6.32-358.78.1.el6
perf-2.6.32-358.78.1.el6
kernel-debuginfo-2.6.32-358.78.1.el6
python-perf-debuginfo-2.6.32-358.78.1.el6
perf-debuginfo-2.6.32-358.78.1.el6
python-perf-2.6.32-358.78.1.el6
kernel-debug-debuginfo-2.6.32-358.78.1.el6
kernel-debug-devel-2.6.32-358.78.1.el6
kernel-debug-2.6.32-358.78.1.el6
kernel-2.6.32-358.78.1.el6
kernel-headers-2.6.32-358.78.1.el6

noarch
kernel-doc-2.6.32-358.78.1.el6
kernel-firmware-2.6.32-358.78.1.el6

141545 - Red Hat Enterprise Linux RHSA-2017-0920 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
RHSA-2017-0920

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00017.html

RHEL7D
x86_64
389-ds-base-1.3.5.10-20.el7_3
389-ds-base-debuginfo-1.3.5.10-20.el7_3
389-ds-base-snmp-1.3.5.10-20.el7_3
389-ds-base-devel-1.3.5.10-20.el7_3
389-ds-base-libs-1.3.5.10-20.el7_3

RHEL7S
x86_64
389-ds-base-1.3.5.10-20.el7_3
389-ds-base-debuginfo-1.3.5.10-20.el7_3
389-ds-base-snmp-1.3.5.10-20.el7_3
389-ds-base-devel-1.3.5.10-20.el7_3
389-ds-base-libs-1.3.5.10-20.el7_3

RHEL7WS
x86_64
389-ds-base-1.3.5.10-20.el7_3
389-ds-base-debuginfo-1.3.5.10-20.el7_3
389-ds-base-snmp-1.3.5.10-20.el7_3
389-ds-base-devel-1.3.5.10-20.el7_3
389-ds-base-libs-1.3.5.10-20.el7_3

145309 - SuSE SLES 11 SP4 SUSE-SU-2017:1008-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1008-1

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-April/002800.html

SuSE SLES 11 SP4
i586
sblim-sfcb-1.3.11-0.28.1

x86_64
sblim-sfcb-1.3.11-0.28.1

145311 - SuSE SLES 11 SP4 SUSE-SU-2017:1027-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3137

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1027-1

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-April/002803.html

SuSE SLES 11 SP4
i586
bind-libs-9.9.6P1-0.47.1
bind-doc-9.9.6P1-0.47.1
bind-9.9.6P1-0.47.1
bind-utils-9.9.6P1-0.47.1
bind-chrootenv-9.9.6P1-0.47.1

x86_64
bind-chrootenv-9.9.6P1-0.47.1
bind-libs-32bit-9.9.6P1-0.47.1
bind-doc-9.9.6P1-0.47.1
bind-libs-9.9.6P1-0.47.1
bind-utils-9.9.6P1-0.47.1
bind-9.9.6P1-0.47.1

160233 - CentOS 7 CESA-2017-0920 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
CESA-2017-0920

Observation

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

For more information see:

http://lists.centos.org/pipermail/centos-announce/2017-April/022370.html

CentOS 7
x86_64
389-ds-base-1.3.5.10-20.el7_3
389-ds-base-snmp-1.3.5.10-20.el7_3
389-ds-base-devel-1.3.5.10-20.el7_3
389-ds-base-libs-1.3.5.10-20.el7_3

160234 - CentOS 7 CESA-2017-0933 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
CESA-2017-0933

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-April/022385.html

CentOS 7
x86_64
perf-3.10.0-514.16.1.el7
kernel-debug-3.10.0-514.16.1.el7
kernel-debug-devel-3.10.0-514.16.1.el7
kernel-tools-libs-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.el7
kernel-3.10.0-514.16.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.el7
kernel-tools-3.10.0-514.16.1.el7
python-perf-3.10.0-514.16.1.el7
kernel-devel-3.10.0-514.16.1.el7

noarch
kernel-abi-whitelists-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.el7

160236 - CentOS 6 CESA-2017-0893 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
CESA-2017-0893

Observation

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

For more information see:

http://lists.centos.org/pipermail/centos-announce/2017-April/022355.html

CentOS 6
x86_64
389-ds-base-devel-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9

i686
389-ds-base-devel-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9

163328 - Oracle Enterprise Linux ELSA-2017-0987 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9603

Description

The scan detected that the host is missing the following update:
ELSA-2017-0987

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006867.html

OEL7
x86_64
qemu-kvm-1.5.3-126.el7_3.6
qemu-kvm-tools-1.5.3-126.el7_3.6
qemu-kvm-common-1.5.3-126.el7_3.6
qemu-img-1.5.3-126.el7_3.6

163332 - Oracle Enterprise Linux ELSA-2017-0920 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
ELSA-2017-0920

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006854.html

OEL7
x86_64

389-ds-base-1.3.5.10-20.el7_3
389-ds-base-snmp-1.3.5.10-20.el7_3
389-ds-base-devel-1.3.5.10-20.el7_3
389-ds-base-libs-1.3.5.10-20.el7_3

163334 - Oracle Enterprise Linux ELSA-2017-0933 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2017-6074

Description

The scan detected that the host is missing the following update:
ELSA-2017-0933

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006830.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006863.html

OEL7
x86_64
kernel-debug-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.el7
python-perf-3.10.0-514.16.1.0.1.el7
kernel-tools-libs-3.10.0-514.16.1.el7
kernel-tools-3.10.0-514.16.1.0.1.el7
kernel-tools-libs-3.10.0-514.16.1.0.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.0.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.0.1.el7
kernel-debug-devel-3.10.0-514.16.1.0.1.el7
kernel-abi-whitelists-3.10.0-514.16.1.el7
perf-3.10.0-514.16.1.0.1.el7
python-perf-3.10.0-514.16.1.el7
kernel-3.10.0-514.16.1.0.1.el7
kernel-devel-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.el7
kernel-devel-3.10.0-514.16.1.0.1.el7
kernel-debug-3.10.0-514.16.1.0.1.el7
kernel-tools-3.10.0-514.16.1.el7
kernel-abi-whitelists-3.10.0-514.16.1.0.1.el7
perf-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.0.1.el7
kernel-3.10.0-514.16.1.el7
kernel-debug-devel-3.10.0-514.16.1.el7

170791 - Amazon Linux AMI ALAS-2017-814 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux 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:
ALAS-2017-814

Observation

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

https://alas.aws.amazon.com/ALAS-2017-814.html

Amazon Linux AMI
i686
kernel-debuginfo-4.9.20-10.30.amzn1
kernel-headers-4.9.20-10.30.amzn1
kernel-tools-4.9.20-10.30.amzn1
kernel-debuginfo-common-i686-4.9.20-10.30.amzn1
kernel-4.9.20-10.30.amzn1
kernel-tools-devel-4.9.20-10.30.amzn1
perf-4.9.20-10.30.amzn1
perf-debuginfo-4.9.20-10.30.amzn1
kernel-devel-4.9.20-10.30.amzn1
kernel-tools-debuginfo-4.9.20-10.30.amzn1

noarch
kernel-doc-4.9.20-10.30.amzn1

x86_64
kernel-debuginfo-common-x86_64-4.9.20-10.30.amzn1
kernel-debuginfo-4.9.20-10.30.amzn1
kernel-tools-4.9.20-10.30.amzn1
kernel-4.9.20-10.30.amzn1
perf-debuginfo-4.9.20-10.30.amzn1
kernel-devel-4.9.20-10.30.amzn1
kernel-tools-devel-4.9.20-10.30.amzn1
perf-4.9.20-10.30.amzn1
kernel-headers-4.9.20-10.30.amzn1
kernel-tools-debuginfo-4.9.20-10.30.amzn1

170792 - Amazon Linux AMI ALAS-2017-815 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8610, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

Description

The scan detected that the host is missing the following update:
ALAS-2017-815

Observation

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

https://alas.aws.amazon.com/ALAS-2017-815.html

Amazon Linux AMI
x86_64
gnutls-guile-2.12.23-21.18.amzn1
gnutls-utils-2.12.23-21.18.amzn1

gnutls-debuginfo-2.12.23-21.18.amzn1
gnutls-devel-2.12.23-21.18.amzn1
gnutls-2.12.23-21.18.amzn1

i686
gnutls-guile-2.12.23-21.18.amzn1
gnutls-utils-2.12.23-21.18.amzn1
gnutls-2.12.23-21.18.amzn1
gnutls-devel-2.12.23-21.18.amzn1
gnutls-debuginfo-2.12.23-21.18.amzn1

175152 - Scientific Linux Security ERRATA Important: 389-ds-base on SL7.x x86_64 (1704-8154)

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: 389-ds-base on SL7.x x86_64 (1704-8154)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=8154

SL7
x86_64
389-ds-base-1.3.5.10-20.el7_3
389-ds-base-debuginfo-1.3.5.10-20.el7_3
389-ds-base-snmp-1.3.5.10-20.el7_3
389-ds-base-devel-1.3.5.10-20.el7_3
389-ds-base-libs-1.3.5.10-20.el7_3

175154 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1704-16606)

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

Risk Level: High

CVE: CVE-2016-9603

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1704-16606)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=16606

SL7
x86_64
qemu-kvm-debuginfo-1.5.3-126.el7_3.6
qemu-kvm-1.5.3-126.el7_3.6
qemu-kvm-tools-1.5.3-126.el7_3.6

qemu-kvm-common-1.5.3-126.el7_3.6
qemu-img-1.5.3-126.el7_3.6

175156 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1704-6692)

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1704-6692)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=6692

SL7
x86_64
kernel-debug-3.10.0-514.16.1.el7
kernel-headers-3.10.0-514.16.1.el7
perf-debuginfo-3.10.0-514.16.1.el7
kernel-tools-libs-devel-3.10.0-514.16.1.el7
kernel-tools-libs-3.10.0-514.16.1.el7
kernel-debug-debuginfo-3.10.0-514.16.1.el7
kernel-debug-devel-3.10.0-514.16.1.el7
kernel-tools-debuginfo-3.10.0-514.16.1.el7
kernel-debuginfo-3.10.0-514.16.1.el7
python-perf-3.10.0-514.16.1.el7
kernel-devel-3.10.0-514.16.1.el7
kernel-tools-3.10.0-514.16.1.el7
kernel-debuginfo-common-x86_64-3.10.0-514.16.1.el7
perf-3.10.0-514.16.1.el7
python-perf-debuginfo-3.10.0-514.16.1.el7
kernel-3.10.0-514.16.1.el7

noarch
kernel-abi-whitelists-3.10.0-514.16.1.el7
kernel-doc-3.10.0-514.16.1.el7

191939 - Fedora Linux 24 FEDORA-2017-8eac23007d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6967

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8eac23007d

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/2017/4/?count=200&page=1

Fedora Core 24

xorgxrdp-0.2.1-1.fc24
xrdp-0.9.2-5.fc24

191946 - Fedora Linux 25 FEDORA-2017-7bd002b77c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6967

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7bd002b77c

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/2017/4/?count=200&page=1

Fedora Core 25

xorgxrdp-0.2.1-1.fc25
xrdp-0.9.2-5.fc25

191949 - Fedora Linux 24 FEDORA-2017-502cf68d68 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2671, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
FEDORA-2017-502cf68d68

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/2017/4/?count=200&page=2

Fedora Core 24

kernel-4.10.9-100.fc24

191952 - Fedora Linux 25 FEDORA-2017-3a9ec92dd6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2671, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3a9ec92dd6

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/2017/4/?count=200&page=2

Fedora Core 25

kernel-4.10.9-200.fc25

191959 - Fedora Linux 24 FEDORA-2017-8e7549fb91 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7308, CVE-2017-7616, CVE-2017-7618

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8e7549fb91

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/2017/4/?count=200&page=1

Fedora Core 24

kernel-4.10.10-100.fc24

191968 - Fedora Linux 25 FEDORA-2017-26c9ecd7a4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7308, CVE-2017-7616, CVE-2017-7618

Description

The scan detected that the host is missing the following update:
FEDORA-2017-26c9ecd7a4

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/2017/4/?count=200&page=1

Fedora Core 25

kernel-4.10.10-200.fc25

191972 - Fedora Linux 26 FEDORA-2017-fc634e7ee7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6967

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fc634e7ee7

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/2017/4/?count=200&page=3

Fedora Core 26

xrdp-0.9.2-5.fc26
xorgxrdp-0.2.1-1.fc26

191974 - Fedora Linux 24 FEDORA-2017-03dc811be6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7228, CVE-2017-7377

Description

The scan detected that the host is missing the following update:
FEDORA-2017-03dc811be6

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/2017/4/?count=200&page=2

Fedora Core 24

xen-4.6.5-5.fc24

21515 - (SYM17-002) Symantec Endpoint Protection Client Multiple Vulnerabilities

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-9093, CVE-2016-9094

Description

Multiple vulnerabilities are present in some versions of Symantec Endpoint Protection.

Observation

Symantec Endpoint Protection enables the management of endpoint nodes of anti-malware for Windows, Mac and Linux computers.

Multiple vulnerabilities are present in some versions of Symantec Endpoint Protection. The flaws lie in several components. Successful exploitation could allow a local attacker to cause a denial of service condition, escalate privileges or execute arbitrary code on the target system.

21703 - Cisco IOS Software Autonomic Networking Infrastructure Registrar Denial Of Service Vulnerability (CSCvc42717)

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

Risk Level: Medium

CVE: CVE-2017-3849

Description

A denial of service vulnerability is present in some versions of Cisco IOS Software.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS Software. The flaw lies in the Autonomic Networking Infrastructure registrar feature. Successful exploitation could allow an attacker to cause a denial of service condition.

141546 - Red Hat Enterprise Linux RHSA-2017-0935 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

Description

The scan detected that the host is missing the following update:
RHSA-2017-0935

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00019.html

RHEL7D
noarch
tomcat-servlet-3.0-api-7.0.69-11.el7_3
tomcat-docs-webapp-7.0.69-11.el7_3
tomcat-el-2.2-api-7.0.69-11.el7_3
tomcat-jsvc-7.0.69-11.el7_3
tomcat-admin-webapps-7.0.69-11.el7_3
tomcat-lib-7.0.69-11.el7_3
tomcat-7.0.69-11.el7_3
tomcat-javadoc-7.0.69-11.el7_3
tomcat-jsp-2.2-api-7.0.69-11.el7_3
tomcat-webapps-7.0.69-11.el7_3

RHEL7S
noarch
tomcat-javadoc-7.0.69-11.el7_3
tomcat-servlet-3.0-api-7.0.69-11.el7_3
tomcat-docs-webapp-7.0.69-11.el7_3
tomcat-jsp-2.2-api-7.0.69-11.el7_3
tomcat-jsvc-7.0.69-11.el7_3
tomcat-admin-webapps-7.0.69-11.el7_3

tomcat-7.0.69-11.el7_3
tomcat-el-2.2-api-7.0.69-11.el7_3
tomcat-lib-7.0.69-11.el7_3
tomcat-webapps-7.0.69-11.el7_3

RHEL7WS
noarch
tomcat-javadoc-7.0.69-11.el7_3
tomcat-servlet-3.0-api-7.0.69-11.el7_3
tomcat-docs-webapp-7.0.69-11.el7_3
tomcat-jsp-2.2-api-7.0.69-11.el7_3
tomcat-jsvc-7.0.69-11.el7_3
tomcat-admin-webapps-7.0.69-11.el7_3
tomcat-7.0.69-11.el7_3
tomcat-el-2.2-api-7.0.69-11.el7_3
tomcat-lib-7.0.69-11.el7_3
tomcat-webapps-7.0.69-11.el7_3

145297 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:1044-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10266, CVE-2016-10267, CVE-2016-10268, CVE-2016-10269, CVE-2016-10270, CVE-2016-10271, CVE-2016-10272

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1044-1

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-April/002810.html

SuSE SLED 12 SP1
x86_64
tiff-debugsource-4.0.7-43.1
libtiff5-debuginfo-32bit-4.0.7-43.1
libtiff5-32bit-4.0.7-43.1
tiff-debuginfo-4.0.7-43.1
libtiff5-4.0.7-43.1
libtiff5-debuginfo-4.0.7-43.1

SuSE SLES 12 SP2
x86_64
tiff-4.0.7-43.1
libtiff5-debuginfo-32bit-4.0.7-43.1
tiff-debugsource-4.0.7-43.1
tiff-debuginfo-4.0.7-43.1
libtiff5-32bit-4.0.7-43.1
libtiff5-4.0.7-43.1
libtiff5-debuginfo-4.0.7-43.1

SuSE SLED 12 SP2
x86_64
tiff-debugsource-4.0.7-43.1
libtiff5-debuginfo-32bit-4.0.7-43.1

libtiff5-32bit-4.0.7-43.1
tiff-debuginfo-4.0.7-43.1
libtiff5-4.0.7-43.1
libtiff5-debuginfo-4.0.7-43.1

SuSE SLES 12 SP1
x86_64
tiff-4.0.7-43.1
libtiff5-debuginfo-32bit-4.0.7-43.1
tiff-debugsource-4.0.7-43.1
tiff-debuginfo-4.0.7-43.1
libtiff5-32bit-4.0.7-43.1
libtiff5-4.0.7-43.1
libtiff5-debuginfo-4.0.7-43.1

145298 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:1048-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9042, CVE-2017-6451, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1048-1

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-April/002812.html

SuSE SLED 12 SP1
x86_64
ntp-doc-4.2.8p10-60.1
ntp-debuginfo-4.2.8p10-60.1
ntp-4.2.8p10-60.1
ntp-debugsource-4.2.8p10-60.1

SuSE SLES 12 SP2
x86_64
ntp-doc-4.2.8p10-60.1
ntp-debuginfo-4.2.8p10-60.1
ntp-4.2.8p10-60.1
ntp-debugsource-4.2.8p10-60.1

SuSE SLED 12 SP2
x86_64
ntp-doc-4.2.8p10-60.1
ntp-debuginfo-4.2.8p10-60.1
ntp-4.2.8p10-60.1
ntp-debugsource-4.2.8p10-60.1

SuSE SLES 12 SP1
x86_64
ntp-doc-4.2.8p10-60.1
ntp-debuginfo-4.2.8p10-60.1
ntp-4.2.8p10-60.1
ntp-debugsource-4.2.8p10-60.1

145303 - SuSE SLES 11 SP4 SUSE-SU-2017:1052-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9042, CVE-2017-6451, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1052-1

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-April/002813.html

SuSE SLES 11 SP4
i586
ntp-doc-4.2.8p10-63.1
ntp-4.2.8p10-63.1

x86_64
ntp-doc-4.2.8p10-63.1
ntp-4.2.8p10-63.1

160231 - CentOS 7 CESA-2017-0935 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

Description

The scan detected that the host is missing the following update:
CESA-2017-0935

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-April/022384.html

CentOS 7
noarch
tomcat-servlet-3.0-api-7.0.69-11.el7_3
tomcat-docs-webapp-7.0.69-11.el7_3
tomcat-el-2.2-api-7.0.69-11.el7_3
tomcat-jsvc-7.0.69-11.el7_3
tomcat-javadoc-7.0.69-11.el7_3
tomcat-jsp-2.2-api-7.0.69-11.el7_3
tomcat-7.0.69-11.el7_3
tomcat-lib-7.0.69-11.el7_3
tomcat-admin-webapps-7.0.69-11.el7_3
tomcat-webapps-7.0.69-11.el7_3

163329 - Oracle Enterprise Linux ELSA-2017-0935 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

Description

The scan detected that the host is missing the following update:
ELSA-2017-0935

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006831.html

OEL7
x86_64
tomcat-servlet-3.0-api-7.0.69-11.el7_3
tomcat-docs-webapp-7.0.69-11.el7_3
tomcat-el-2.2-api-7.0.69-11.el7_3
tomcat-jsvc-7.0.69-11.el7_3
tomcat-javadoc-7.0.69-11.el7_3
tomcat-jsp-2.2-api-7.0.69-11.el7_3
tomcat-7.0.69-11.el7_3
tomcat-lib-7.0.69-11.el7_3
tomcat-admin-webapps-7.0.69-11.el7_3
tomcat-webapps-7.0.69-11.el7_3

163333 - Oracle Enterprise Linux ELSA-2017-0914 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4324, CVE-2017-3157

Description

The scan detected that the host is missing the following update:
ELSA-2017-0914

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006841.html

OEL7
x86_64
libreoffice-langpack-gl-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-af-5.0.6.2-5.0.1.el7_3.1
autocorr-lb-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-fi-5.0.6.2-5.0.1.el7_3.1
autocorr-es-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-it-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-sl-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-or-5.0.6.2-5.0.1.el7_3.1
autocorr-sr-5.0.6.2-5.0.1.el7_3.1
autocorr-bg-5.0.6.2-5.0.1.el7_3.1

libreoffice-langpack-nl-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-nb-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-pa-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ja-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-tr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-nr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-lt-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-uk-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-kk-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-hr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-nn-5.0.6.2-5.0.1.el7_3.1
autocorr-fr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-mr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-xh-5.0.6.2-5.0.1.el7_3.1
libreoffice-pdfimport-5.0.6.2-5.0.1.el7_3.1
autocorr-da-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ta-5.0.6.2-5.0.1.el7_3.1
autocorr-cs-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-br-5.0.6.2-5.0.1.el7_3.1
libreoffice-sdk-doc-5.0.6.2-5.0.1.el7_3.1
libreoffice-officebean-5.0.6.2-5.0.1.el7_3.1
autocorr-de-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ml-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-gu-5.0.6.2-5.0.1.el7_3.1
autocorr-mn-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-kn-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-si-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-bn-5.0.6.2-5.0.1.el7_3.1
libreoffice-postgresql-5.0.6.2-5.0.1.el7_3.1
libreoffice-librelogo-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-as-5.0.6.2-5.0.1.el7_3.1
autocorr-pl-5.0.6.2-5.0.1.el7_3.1
autocorr-pt-5.0.6.2-5.0.1.el7_3.1
libreoffice-gdb-debug-support-5.0.6.2-5.0.1.el7_3.1
autocorr-nl-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-he-5.0.6.2-5.0.1.el7_3.1
libreoffice-core-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-lv-5.0.6.2-5.0.1.el7_3.1
autocorr-ga-5.0.6.2-5.0.1.el7_3.1
libreoffice-graphicfilter-5.0.6.2-5.0.1.el7_3.1
libreoffice-emailmerge-5.0.6.2-5.0.1.el7_3.1
autocorr-af-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-hu-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-nso-5.0.6.2-5.0.1.el7_3.1
autocorr-hu-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-eu-5.0.6.2-5.0.1.el7_3.1
autocorr-zh-5.0.6.2-5.0.1.el7_3.1
libreoffice-ure-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-es-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ss-5.0.6.2-5.0.1.el7_3.1
libreoffice-sdk-5.0.6.2-5.0.1.el7_3.1
libreoffice-pyuno-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-pt-PT-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ru-5.0.6.2-5.0.1.el7_3.1
autocorr-vi-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ca-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-el-5.0.6.2-5.0.1.el7_3.1
autocorr-ja-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ko-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ar-5.0.6.2-5.0.1.el7_3.1

libreoffice-langpack-te-5.0.6.2-5.0.1.el7_3.1
libreoffice-nlpsolver-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ro-5.0.6.2-5.0.1.el7_3.1
autocorr-tr-5.0.6.2-5.0.1.el7_3.1
libreoffice-draw-5.0.6.2-5.0.1.el7_3.1
autocorr-sk-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-fr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-st-5.0.6.2-5.0.1.el7_3.1
autocorr-fa-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ga-5.0.6.2-5.0.1.el7_3.1
autocorr-ko-5.0.6.2-5.0.1.el7_3.1
autocorr-ro-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-pl-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-et-5.0.6.2-5.0.1.el7_3.1
libreoffice-bsh-5.0.6.2-5.0.1.el7_3.1
libreoffice-opensymbol-fonts-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-hi-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-sk-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-cy-5.0.6.2-5.0.1.el7_3.1
autocorr-hr-5.0.6.2-5.0.1.el7_3.1
autocorr-sl-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-fa-5.0.6.2-5.0.1.el7_3.1
libreoffice-impress-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-en-5.0.6.2-5.0.1.el7_3.1
autocorr-ca-5.0.6.2-5.0.1.el7_3.1
libreoffice-base-5.0.6.2-5.0.1.el7_3.1
autocorr-en-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-bg-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-mai-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-pt-BR-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-da-5.0.6.2-5.0.1.el7_3.1
autocorr-it-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-th-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-sv-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-zh-Hans-5.0.6.2-5.0.1.el7_3.1
autocorr-ru-5.0.6.2-5.0.1.el7_3.1
libreoffice-filters-5.0.6.2-5.0.1.el7_3.1
libreoffice-glade-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ve-5.0.6.2-5.0.1.el7_3.1
libreoffice-ogltrans-5.0.6.2-5.0.1.el7_3.1
libreoffice-xsltfilter-5.0.6.2-5.0.1.el7_3.1
autocorr-sv-5.0.6.2-5.0.1.el7_3.1
libreoffice-rhino-5.0.6.2-5.0.1.el7_3.1
libreoffice-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-ts-5.0.6.2-5.0.1.el7_3.1
libreoffice-wiki-publisher-5.0.6.2-5.0.1.el7_3.1
autocorr-is-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-sr-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-cs-5.0.6.2-5.0.1.el7_3.1
autocorr-fi-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-tn-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-de-5.0.6.2-5.0.1.el7_3.1
libreoffice-writer-5.0.6.2-5.0.1.el7_3.1
autocorr-lt-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-zh-Hant-5.0.6.2-5.0.1.el7_3.1
libreoffice-math-5.0.6.2-5.0.1.el7_3.1
libreoffice-calc-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-dz-5.0.6.2-5.0.1.el7_3.1
libreoffice-langpack-zu-5.0.6.2-5.0.1.el7_3.1

175158 - Scientific Linux Security ERRATA Moderate: tomcat on SL7.x (noarch) (1704-8502)

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

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: tomcat on SL7.x (noarch) (1704-8502)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=8502

SL7
noarch
tomcat-servlet-3.0-api-7.0.69-11.el7_3
tomcat-docs-webapp-7.0.69-11.el7_3
tomcat-el-2.2-api-7.0.69-11.el7_3
tomcat-jsvc-7.0.69-11.el7_3
tomcat-admin-webapps-7.0.69-11.el7_3
tomcat-lib-7.0.69-11.el7_3
tomcat-7.0.69-11.el7_3
tomcat-javadoc-7.0.69-11.el7_3
tomcat-jsp-2.2-api-7.0.69-11.el7_3
tomcat-webapps-7.0.69-11.el7_3

191940 - Fedora Linux 24 FEDORA-2017-ed6b6a1d7a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9264, CVE-2016-9265, CVE-2016-9266, CVE-2016-9827, CVE-2016-9828, CVE-2016-9829, CVE-2016-9831, CVE-2017-7578

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ed6b6a1d7a

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/2017/4/?count=200&page=1

Fedora Core 24

ming-0.4.8-1.fc24

191943 - Fedora Linux 24 FEDORA-2017-72323a442f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6451, CVE-2017-6458, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
FEDORA-2017-72323a442f

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/2017/4/?count=200&page=1

Fedora Core 24

ntp-4.2.6p5-44.fc24

191944 - Fedora Linux 26 FEDORA-2017-d95dacdfbf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7592, CVE-2017-7593, CVE-2017-7594, CVE-2017-7595, CVE-2017-7596, CVE-2017-7597, CVE-2017-7598, CVE-2017-7599, CVE-2017-7600, CVE-2017-7601, CVE-2017-7602

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d95dacdfbf

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/2017/4/?count=200&page=2

Fedora Core 26

libtiff-4.0.7-5.fc26

191951 - Fedora Linux 26 FEDORA-2017-198ca8ba07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9264, CVE-2016-9265, CVE-2016-9266, CVE-2016-9827, CVE-2016-9828, CVE-2016-9829, CVE-2016-9831, CVE-2017-7578

Description

The scan detected that the host is missing the following update:
FEDORA-2017-198ca8ba07

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/2017/4/?count=200&page=2

Fedora Core 26

ming-0.4.8-1.fc26

191956 - Fedora Linux 25 FEDORA-2017-ae1fde5fb8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5182, CVE-2016-5183, CVE-2016-5189, CVE-2016-5199, CVE-2016-5201, CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-9650, CVE-2016-9651

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ae1fde5fb8

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/2017/4/?count=200&page=1

Fedora Core 25

qt5-qtwebengine-5.8.0-8.fc25

191963 - Fedora Linux 25 FEDORA-2017-021bebae25 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7592, CVE-2017-7593, CVE-2017-7594, CVE-2017-7595, CVE-2017-7596, CVE-2017-7597, CVE-2017-7598, CVE-2017-7599, CVE-2017-7600, CVE-2017-7601, CVE-2017-7602

Description

The scan detected that the host is missing the following update:
FEDORA-2017-021bebae25

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/2017/4/?count=200&page=2

Fedora Core 25

libtiff-4.0.7-5.fc25

191966 - Fedora Linux 26 FEDORA-2017-c5b2c9a435 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5182, CVE-2016-5183, CVE-2016-5189, CVE-2016-5199, CVE-2016-5201, CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-9650, CVE-2016-9651

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c5b2c9a435

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/2017/4/?count=200&page=1

Fedora Core 26

qt5-qtwebengine-5.8.0-8.fc26

21643 - Novell iManager Vulnerabilities Prior To 3.0.3

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2017-5189

Description

Multiple vulnerabilities are present in some versions of Novell (NetIQ) iManager.

Observation

Novell iManager is a web-based administration console.

Multiple vulnerabilities are present in some versions of Novell (NetIQ) iManager. The flaws lie in Tomcat and another unspecified component. Successful exploitation could allow an attacker to recover encrypted plain texts.

21663 - Novell eDirectory Multiple Components Vulnerability Prior To 9.0.3

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2016-7055, CVE-2017-3731, CVE-2017-3732

Description

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory.

Observation

Novell (NetIQ) eDirectory is an X.500 compatible directory service software for centrally managing access to network resources.

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory. The flaws lie in multiple components. Successful exploitation could allow a malicious user to obtain sensitive information, cause a denial-of-service or other unspecified impact.

21688 - Oracle VM VirtualBox Critical Patch Update April 2017

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

Risk Level: Medium

CVE: CVE-2017-3513, CVE-2017-3538, CVE-2017-3558, CVE-2017-3559, CVE-2017-3561, CVE-2017-3563, CVE-2017-3575, CVE-2017-3576, CVE-2017-3587

Description

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox.

Observation

Oracle VM VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox. The flaws exist in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or do unauthorized modifications on the target system.

37563 - IBM AIX IV91362 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
IV91362

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91362

6100-09
bos.net.tcp.client < 6.1.9.201

37564 - IBM AIX IV91363 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
IV91363

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91363

7100-03
bos.net.tcp.client < 7.1.3.49

37565 - IBM AIX IV91364 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
IV91364

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91364

7100-04
bos.net.tcp.client < 7.1.4.31

37566 - IBM AIX IV91366 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
IV91366

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91366

7200-00
bos.net.tcp.bind_utils < 7.2.0.3

37567 - IBM AIX IV91367 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
IV91367

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91367

7200-01
bos.net.tcp.bind_utils < 7.2.1.2

37581 - IBM AIX IV93361 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131

Description

The scan detected that the host is missing the following update:
IV93361

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV93361

6100-09
bos.net.tcp.client < 6.1.9.201

37582 - IBM AIX IV93362 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131

Description

The scan detected that the host is missing the following update:
IV93362

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV93362

7100-03
bos.net.tcp.client < 7.1.3.49

37583 - IBM AIX IV93363 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131

Description

The scan detected that the host is missing the following update:
IV93363

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV93363

7100-04
bos.net.tcp.client < 7.1.4.31

37584 - IBM AIX IV93365 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131

Description

The scan detected that the host is missing the following update:
IV93365

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV93365

7200-01
bos.net.tcp.bind_utils < 7.2.1.2

37585 - IBM AIX IV93403 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131

Description

The scan detected that the host is missing the following update:
IV93403

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV93403

7200-00
bos.net.tcp.bind_utils < 7.2.0.3

141537 - Red Hat Enterprise Linux RHSA-2017-0979 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
RHSA-2017-0979

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00028.html

RHEL6S

i386
libreoffice-langpack-cy-4.3.7.2-2.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.el6_9.1
libreoffice-core-4.3.7.2-2.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.el6_9.1
libreoffice-glade-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.el6_9.1
libreoffice-langpack-ar-4.3.7.2-2.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.el6_9.1
libreoffice-langpack-ta-4.3.7.2-2.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.el6_9.1
libreoffice-calc-4.3.7.2-2.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.el6_9.1
libreoffice-base-4.3.7.2-2.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.el6_9.1
libreoffice-sdk-4.3.7.2-2.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.el6_9.1
libreoffice-writer-4.3.7.2-2.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.el6_9.1
libreoffice-langpack-en-4.3.7.2-2.el6_9.1
libreoffice-pdfimport-4.3.7.2-2.el6_9.1
libreoffice-langpack-ve-4.3.7.2-2.el6_9.1
libreoffice-langpack-nr-4.3.7.2-2.el6_9.1
libreoffice-langpack-fi-4.3.7.2-2.el6_9.1
libreoffice-langpack-th-4.3.7.2-2.el6_9.1
libreoffice-4.3.7.2-2.el6_9.1
libreoffice-impress-4.3.7.2-2.el6_9.1
libreoffice-langpack-eu-4.3.7.2-2.el6_9.1
libreoffice-langpack-ko-4.3.7.2-2.el6_9.1
libreoffice-headless-4.3.7.2-2.el6_9.1

libreoffice-bsh-4.3.7.2-2.el6_9.1
libreoffice-langpack-pa-4.3.7.2-2.el6_9.1
libreoffice-wiki-publisher-4.3.7.2-2.el6_9.1
libreoffice-langpack-mai-4.3.7.2-2.el6_9.1
libreoffice-debuginfo-4.3.7.2-2.el6_9.1
libreoffice-langpack-gl-4.3.7.2-2.el6_9.1
libreoffice-langpack-te-4.3.7.2-2.el6_9.1
libreoffice-langpack-nl-4.3.7.2-2.el6_9.1
libreoffice-pyuno-4.3.7.2-2.el6_9.1
libreoffice-langpack-el-4.3.7.2-2.el6_9.1
libreoffice-langpack-tn-4.3.7.2-2.el6_9.1
libreoffice-langpack-ur-4.3.7.2-2.el6_9.1
libreoffice-langpack-sr-4.3.7.2-2.el6_9.1
libreoffice-ogltrans-4.3.7.2-2.el6_9.1
libreoffice-langpack-tr-4.3.7.2-2.el6_9.1
libreoffice-emailmerge-4.3.7.2-2.el6_9.1
libreoffice-sdk-doc-4.3.7.2-2.el6_9.1
libreoffice-filters-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-PT-4.3.7.2-2.el6_9.1
libreoffice-langpack-or-4.3.7.2-2.el6_9.1
libreoffice-langpack-kn-4.3.7.2-2.el6_9.1
libreoffice-ure-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hans-4.3.7.2-2.el6_9.1
libreoffice-draw-4.3.7.2-2.el6_9.1
libreoffice-langpack-mr-4.3.7.2-2.el6_9.1
libreoffice-nlpsolver-4.3.7.2-2.el6_9.1
libreoffice-officebean-4.3.7.2-2.el6_9.1
libreoffice-langpack-pl-4.3.7.2-2.el6_9.1
libreoffice-librelogo-4.3.7.2-2.el6_9.1
libreoffice-langpack-hr-4.3.7.2-2.el6_9.1
libreoffice-rhino-4.3.7.2-2.el6_9.1
libreoffice-langpack-de-4.3.7.2-2.el6_9.1
libreoffice-math-4.3.7.2-2.el6_9.1
libreoffice-langpack-hu-4.3.7.2-2.el6_9.1

noarch
autocorr-pl-4.3.7.2-2.el6_9.1
autocorr-cs-4.3.7.2-2.el6_9.1
autocorr-ro-4.3.7.2-2.el6_9.1
autocorr-hr-4.3.7.2-2.el6_9.1
autocorr-tr-4.3.7.2-2.el6_9.1
autocorr-de-4.3.7.2-2.el6_9.1
autocorr-sl-4.3.7.2-2.el6_9.1
autocorr-ga-4.3.7.2-2.el6_9.1
autocorr-lb-4.3.7.2-2.el6_9.1
autocorr-vi-4.3.7.2-2.el6_9.1
autocorr-sr-4.3.7.2-2.el6_9.1
autocorr-en-4.3.7.2-2.el6_9.1
libreoffice-opensymbol-fonts-4.3.7.2-2.el6_9.1
autocorr-sv-4.3.7.2-2.el6_9.1
autocorr-da-4.3.7.2-2.el6_9.1
autocorr-lt-4.3.7.2-2.el6_9.1
autocorr-fa-4.3.7.2-2.el6_9.1
autocorr-hu-4.3.7.2-2.el6_9.1
autocorr-nl-4.3.7.2-2.el6_9.1
autocorr-ca-4.3.7.2-2.el6_9.1
autocorr-pt-4.3.7.2-2.el6_9.1
autocorr-ko-4.3.7.2-2.el6_9.1
autocorr-ru-4.3.7.2-2.el6_9.1
autocorr-is-4.3.7.2-2.el6_9.1

autocorr-ja-4.3.7.2-2.el6_9.1
autocorr-sk-4.3.7.2-2.el6_9.1
autocorr-zh-4.3.7.2-2.el6_9.1
autocorr-mn-4.3.7.2-2.el6_9.1
autocorr-it-4.3.7.2-2.el6_9.1
autocorr-es-4.3.7.2-2.el6_9.1
autocorr-af-4.3.7.2-2.el6_9.1
autocorr-fr-4.3.7.2-2.el6_9.1
autocorr-bg-4.3.7.2-2.el6_9.1
autocorr-fi-4.3.7.2-2.el6_9.1

x86_64
libreoffice-langpack-cy-4.3.7.2-2.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.el6_9.1
libreoffice-core-4.3.7.2-2.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.el6_9.1
libreoffice-glade-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.el6_9.1
libreoffice-langpack-ar-4.3.7.2-2.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.el6_9.1
libreoffice-langpack-ta-4.3.7.2-2.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.el6_9.1
libreoffice-calc-4.3.7.2-2.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.el6_9.1
libreoffice-base-4.3.7.2-2.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.el6_9.1
libreoffice-sdk-4.3.7.2-2.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.el6_9.1
libreoffice-writer-4.3.7.2-2.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.el6_9.1

RHEL6D
i386
libreoffice-langpack-cy-4.3.7.2-2.el6_9.1

RHEL6WS
i386
libreoffice-langpack-cy-4.3.7.2-2.el6_9.1

141538 - Red Hat Enterprise Linux RHSA-2017-0907 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
RHSA-2017-0907

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00015.html

RHEL7D
x86_64
libuuid-2.23.2-33.el7_3.2
libblkid-devel-2.23.2-33.el7_3.2
libuuid-devel-2.23.2-33.el7_3.2
libblkid-2.23.2-33.el7_3.2
libmount-2.23.2-33.el7_3.2
uuidd-2.23.2-33.el7_3.2
util-linux-2.23.2-33.el7_3.2
libmount-devel-2.23.2-33.el7_3.2
util-linux-debuginfo-2.23.2-33.el7_3.2

RHEL7S
x86_64
libuuid-2.23.2-33.el7_3.2
libuuid-devel-2.23.2-33.el7_3.2
libblkid-devel-2.23.2-33.el7_3.2
libblkid-2.23.2-33.el7_3.2
libmount-2.23.2-33.el7_3.2
uuidd-2.23.2-33.el7_3.2
util-linux-2.23.2-33.el7_3.2
libmount-devel-2.23.2-33.el7_3.2
util-linux-debuginfo-2.23.2-33.el7_3.2

RHEL7WS
x86_64
libuuid-2.23.2-33.el7_3.2
libuuid-devel-2.23.2-33.el7_3.2
libblkid-devel-2.23.2-33.el7_3.2
libblkid-2.23.2-33.el7_3.2
libmount-2.23.2-33.el7_3.2
uuidd-2.23.2-33.el7_3.2
util-linux-2.23.2-33.el7_3.2
libmount-devel-2.23.2-33.el7_3.2

util-linux-debuginfo-2.23.2-33.el7_3.2

141541 - Red Hat Enterprise Linux RHSA-2017-0906 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
RHSA-2017-0906

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00014.html

RHEL7D
x86_64
mod_ldap-2.4.6-45.el7_3.4
httpd-debuginfo-2.4.6-45.el7_3.4
mod_session-2.4.6-45.el7_3.4
mod_proxy_html-2.4.6-45.el7_3.4
httpd-2.4.6-45.el7_3.4
httpd-tools-2.4.6-45.el7_3.4
httpd-devel-2.4.6-45.el7_3.4
mod_ssl-2.4.6-45.el7_3.4

noarch
httpd-manual-2.4.6-45.el7_3.4

RHEL7S
noarch
httpd-manual-2.4.6-45.el7_3.4

x86_64
mod_ssl-2.4.6-45.el7_3.4
httpd-debuginfo-2.4.6-45.el7_3.4
mod_ldap-2.4.6-45.el7_3.4
mod_proxy_html-2.4.6-45.el7_3.4
httpd-2.4.6-45.el7_3.4
httpd-tools-2.4.6-45.el7_3.4
httpd-devel-2.4.6-45.el7_3.4
mod_session-2.4.6-45.el7_3.4

RHEL7WS
x86_64
mod_ssl-2.4.6-45.el7_3.4
httpd-debuginfo-2.4.6-45.el7_3.4
mod_ldap-2.4.6-45.el7_3.4
mod_proxy_html-2.4.6-45.el7_3.4
httpd-2.4.6-45.el7_3.4
httpd-tools-2.4.6-45.el7_3.4
httpd-devel-2.4.6-45.el7_3.4
mod_session-2.4.6-45.el7_3.4

noarch

httpd-manual-2.4.6-45.el7_3.4

141543 - Red Hat Enterprise Linux RHSA-2017-0914 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
RHSA-2017-0914

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00016.html

RHEL7D
x86_64
libreoffice-graphicfilter-5.0.6.2-5.el7_3.1
libreoffice-debuginfo-5.0.6.2-5.el7_3.1
libreoffice-langpack-gl-5.0.6.2-5.el7_3.1
libreoffice-langpack-it-5.0.6.2-5.el7_3.1
libreoffice-langpack-ga-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hant-5.0.6.2-5.el7_3.1
libreoffice-langpack-xh-5.0.6.2-5.el7_3.1
libreoffice-langpack-ca-5.0.6.2-5.el7_3.1
libreoffice-langpack-lt-5.0.6.2-5.el7_3.1
libreoffice-langpack-ss-5.0.6.2-5.el7_3.1
libreoffice-langpack-zu-5.0.6.2-5.el7_3.1
libreoffice-langpack-st-5.0.6.2-5.el7_3.1
libreoffice-langpack-fi-5.0.6.2-5.el7_3.1
libreoffice-ogltrans-5.0.6.2-5.el7_3.1
libreoffice-langpack-gu-5.0.6.2-5.el7_3.1
libreoffice-base-5.0.6.2-5.el7_3.1
libreoffice-langpack-kk-5.0.6.2-5.el7_3.1
libreoffice-langpack-th-5.0.6.2-5.el7_3.1
libreoffice-ure-5.0.6.2-5.el7_3.1
libreoffice-langpack-eu-5.0.6.2-5.el7_3.1
libreoffice-calc-5.0.6.2-5.el7_3.1
libreoffice-sdk-doc-5.0.6.2-5.el7_3.1
libreoffice-langpack-nl-5.0.6.2-5.el7_3.1
libreoffice-langpack-pt-PT-5.0.6.2-5.el7_3.1
libreoffice-langpack-el-5.0.6.2-5.el7_3.1
libreoffice-langpack-si-5.0.6.2-5.el7_3.1
libreoffice-rhino-5.0.6.2-5.el7_3.1
libreoffice-langpack-ru-5.0.6.2-5.el7_3.1
libreoffice-5.0.6.2-5.el7_3.1
libreoffice-langpack-bn-5.0.6.2-5.el7_3.1
libreoffice-langpack-ja-5.0.6.2-5.el7_3.1
libreoffice-langpack-nso-5.0.6.2-5.el7_3.1
libreoffice-langpack-hi-5.0.6.2-5.el7_3.1
libreoffice-langpack-nb-5.0.6.2-5.el7_3.1
libreoffice-langpack-kn-5.0.6.2-5.el7_3.1
libreoffice-langpack-cy-5.0.6.2-5.el7_3.1
libreoffice-langpack-es-5.0.6.2-5.el7_3.1
libreoffice-langpack-nr-5.0.6.2-5.el7_3.1

libreoffice-langpack-ro-5.0.6.2-5.el7_3.1
libreoffice-wiki-publisher-5.0.6.2-5.el7_3.1
libreoffice-gdb-debug-support-5.0.6.2-5.el7_3.1
libreoffice-langpack-uk-5.0.6.2-5.el7_3.1
libreoffice-langpack-sk-5.0.6.2-5.el7_3.1
libreoffice-langpack-tr-5.0.6.2-5.el7_3.1
libreoffice-langpack-ta-5.0.6.2-5.el7_3.1
libreoffice-langpack-dz-5.0.6.2-5.el7_3.1
libreoffice-langpack-sl-5.0.6.2-5.el7_3.1
libreoffice-langpack-fa-5.0.6.2-5.el7_3.1
libreoffice-writer-5.0.6.2-5.el7_3.1
libreoffice-postgresql-5.0.6.2-5.el7_3.1
libreoffice-langpack-ar-5.0.6.2-5.el7_3.1
libreoffice-langpack-or-5.0.6.2-5.el7_3.1
libreoffice-pyuno-5.0.6.2-5.el7_3.1
libreoffice-langpack-pl-5.0.6.2-5.el7_3.1
libreoffice-langpack-te-5.0.6.2-5.el7_3.1
libreoffice-langpack-pa-5.0.6.2-5.el7_3.1
libreoffice-xsltfilter-5.0.6.2-5.el7_3.1
libreoffice-langpack-mr-5.0.6.2-5.el7_3.1
libreoffice-sdk-5.0.6.2-5.el7_3.1
libreoffice-draw-5.0.6.2-5.el7_3.1
libreoffice-librelogo-5.0.6.2-5.el7_3.1
libreoffice-langpack-mai-5.0.6.2-5.el7_3.1
libreoffice-langpack-ml-5.0.6.2-5.el7_3.1
libreoffice-langpack-hu-5.0.6.2-5.el7_3.1
libreoffice-core-5.0.6.2-5.el7_3.1
libreoffice-langpack-sr-5.0.6.2-5.el7_3.1
libreoffice-emailmerge-5.0.6.2-5.el7_3.1
libreoffice-langpack-da-5.0.6.2-5.el7_3.1
libreoffice-langpack-sv-5.0.6.2-5.el7_3.1
libreoffice-langpack-af-5.0.6.2-5.el7_3.1
libreoffice-langpack-de-5.0.6.2-5.el7_3.1
libreoffice-langpack-cs-5.0.6.2-5.el7_3.1
libreoffice-langpack-tn-5.0.6.2-5.el7_3.1
libreoffice-langpack-ve-5.0.6.2-5.el7_3.1
libreoffice-filters-5.0.6.2-5.el7_3.1
libreoffice-langpack-he-5.0.6.2-5.el7_3.1
libreoffice-langpack-et-5.0.6.2-5.el7_3.1
libreoffice-nlpsolver-5.0.6.2-5.el7_3.1
libreoffice-bsh-5.0.6.2-5.el7_3.1
libreoffice-langpack-nn-5.0.6.2-5.el7_3.1
libreoffice-langpack-bg-5.0.6.2-5.el7_3.1
libreoffice-langpack-en-5.0.6.2-5.el7_3.1
libreoffice-langpack-ts-5.0.6.2-5.el7_3.1
libreoffice-langpack-pt-BR-5.0.6.2-5.el7_3.1
libreoffice-langpack-lv-5.0.6.2-5.el7_3.1
libreoffice-langpack-hr-5.0.6.2-5.el7_3.1
libreoffice-glade-5.0.6.2-5.el7_3.1
libreoffice-officebean-5.0.6.2-5.el7_3.1
libreoffice-impress-5.0.6.2-5.el7_3.1
libreoffice-langpack-fr-5.0.6.2-5.el7_3.1
libreoffice-math-5.0.6.2-5.el7_3.1
libreoffice-pdfimport-5.0.6.2-5.el7_3.1
libreoffice-langpack-ko-5.0.6.2-5.el7_3.1
libreoffice-langpack-br-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hans-5.0.6.2-5.el7_3.1
libreoffice-langpack-as-5.0.6.2-5.el7_3.1

noarch

autocorr-ja-5.0.6.2-5.el7_3.1
autocorr-cs-5.0.6.2-5.el7_3.1
autocorr-it-5.0.6.2-5.el7_3.1
autocorr-hr-5.0.6.2-5.el7_3.1
autocorr-fa-5.0.6.2-5.el7_3.1
autocorr-ro-5.0.6.2-5.el7_3.1
autocorr-fi-5.0.6.2-5.el7_3.1
autocorr-pl-5.0.6.2-5.el7_3.1
autocorr-vi-5.0.6.2-5.el7_3.1
autocorr-zh-5.0.6.2-5.el7_3.1
autocorr-lb-5.0.6.2-5.el7_3.1
autocorr-sv-5.0.6.2-5.el7_3.1
autocorr-sr-5.0.6.2-5.el7_3.1
autocorr-en-5.0.6.2-5.el7_3.1
autocorr-mn-5.0.6.2-5.el7_3.1
autocorr-hu-5.0.6.2-5.el7_3.1
autocorr-ga-5.0.6.2-5.el7_3.1
autocorr-tr-5.0.6.2-5.el7_3.1
autocorr-de-5.0.6.2-5.el7_3.1
libreoffice-opensymbol-fonts-5.0.6.2-5.el7_3.1
autocorr-sk-5.0.6.2-5.el7_3.1
autocorr-fr-5.0.6.2-5.el7_3.1
autocorr-nl-5.0.6.2-5.el7_3.1
autocorr-is-5.0.6.2-5.el7_3.1
autocorr-da-5.0.6.2-5.el7_3.1
autocorr-af-5.0.6.2-5.el7_3.1
autocorr-ko-5.0.6.2-5.el7_3.1
autocorr-bg-5.0.6.2-5.el7_3.1
autocorr-sl-5.0.6.2-5.el7_3.1
autocorr-es-5.0.6.2-5.el7_3.1
autocorr-pt-5.0.6.2-5.el7_3.1
autocorr-ca-5.0.6.2-5.el7_3.1
autocorr-ru-5.0.6.2-5.el7_3.1
autocorr-lt-5.0.6.2-5.el7_3.1

RHEL7S
noarch
autocorr-ja-5.0.6.2-5.el7_3.1
autocorr-cs-5.0.6.2-5.el7_3.1
autocorr-it-5.0.6.2-5.el7_3.1
autocorr-hr-5.0.6.2-5.el7_3.1
autocorr-fa-5.0.6.2-5.el7_3.1
autocorr-ro-5.0.6.2-5.el7_3.1
autocorr-fi-5.0.6.2-5.el7_3.1
autocorr-pl-5.0.6.2-5.el7_3.1
autocorr-vi-5.0.6.2-5.el7_3.1
autocorr-zh-5.0.6.2-5.el7_3.1
autocorr-lb-5.0.6.2-5.el7_3.1
autocorr-sv-5.0.6.2-5.el7_3.1
autocorr-sr-5.0.6.2-5.el7_3.1
autocorr-en-5.0.6.2-5.el7_3.1
autocorr-mn-5.0.6.2-5.el7_3.1
autocorr-hu-5.0.6.2-5.el7_3.1
autocorr-ga-5.0.6.2-5.el7_3.1
autocorr-tr-5.0.6.2-5.el7_3.1
autocorr-de-5.0.6.2-5.el7_3.1
libreoffice-opensymbol-fonts-5.0.6.2-5.el7_3.1
autocorr-sk-5.0.6.2-5.el7_3.1
autocorr-fr-5.0.6.2-5.el7_3.1
autocorr-nl-5.0.6.2-5.el7_3.1

autocorr-is-5.0.6.2-5.el7_3.1
autocorr-da-5.0.6.2-5.el7_3.1
autocorr-af-5.0.6.2-5.el7_3.1
autocorr-ko-5.0.6.2-5.el7_3.1
autocorr-bg-5.0.6.2-5.el7_3.1
autocorr-sl-5.0.6.2-5.el7_3.1
autocorr-es-5.0.6.2-5.el7_3.1
autocorr-pt-5.0.6.2-5.el7_3.1
autocorr-ca-5.0.6.2-5.el7_3.1
autocorr-ru-5.0.6.2-5.el7_3.1
autocorr-lt-5.0.6.2-5.el7_3.1

x86_64
libreoffice-graphicfilter-5.0.6.2-5.el7_3.1
libreoffice-debuginfo-5.0.6.2-5.el7_3.1
libreoffice-langpack-gl-5.0.6.2-5.el7_3.1
libreoffice-langpack-it-5.0.6.2-5.el7_3.1
libreoffice-langpack-ga-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hant-5.0.6.2-5.el7_3.1
libreoffice-langpack-xh-5.0.6.2-5.el7_3.1
libreoffice-langpack-ca-5.0.6.2-5.el7_3.1
libreoffice-langpack-lt-5.0.6.2-5.el7_3.1
libreoffice-langpack-da-5.0.6.2-5.el7_3.1
libreoffice-langpack-de-5.0.6.2-5.el7_3.1
libreoffice-langpack-fi-5.0.6.2-5.el7_3.1
libreoffice-ogltrans-5.0.6.2-5.el7_3.1
libreoffice-langpack-gu-5.0.6.2-5.el7_3.1
libreoffice-base-5.0.6.2-5.el7_3.1
libreoffice-langpack-kk-5.0.6.2-5.el7_3.1
libreoffice-langpack-th-5.0.6.2-5.el7_3.1
libreoffice-ure-5.0.6.2-5.el7_3.1
libreoffice-langpack-nr-5.0.6.2-5.el7_3.1

RHEL7WS
x86_64
libreoffice-graphicfilter-5.0.6.2-5.el7_3.1

145300 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1010-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2017-5840, CVE-2017-5841, CVE-2017-5845

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1010-1

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-April/002801.html

SuSE SLED 12 SP2
x86_64
gstreamer-plugins-good-debuginfo-1.8.3-12.12
gstreamer-plugins-good-debugsource-1.8.3-12.12
gstreamer-plugins-good-1.8.3-12.12

noarch
gstreamer-plugins-good-lang-1.8.3-12.12

SuSE SLES 12 SP2
noarch
gstreamer-plugins-good-lang-1.8.3-12.12

x86_64
gstreamer-plugins-good-debuginfo-1.8.3-12.12
gstreamer-plugins-good-debugsource-1.8.3-12.12
gstreamer-plugins-good-1.8.3-12.12

145307 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:1004-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2017-5840

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1004-1

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-April/002799.html

SuSE SLES 12 SP1
noarch
gstreamer-plugins-good-lang-1.2.4-2.9.1

x86_64
gstreamer-plugins-good-debugsource-1.2.4-2.9.1
gstreamer-plugins-good-debuginfo-1.2.4-2.9.1
gstreamer-plugins-good-1.2.4-2.9.1

SuSE SLED 12 SP1
x86_64
gstreamer-plugins-good-debugsource-1.2.4-2.9.1
gstreamer-plugins-good-debuginfo-1.2.4-2.9.1
gstreamer-plugins-good-1.2.4-2.9.1

noarch
gstreamer-plugins-good-lang-1.2.4-2.9.1

145310 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:1041-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5839, CVE-2017-5842, CVE-2017-5844

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1041-1

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-April/002807.html

SuSE SLES 12 SP1
noarch
gstreamer-plugins-base-lang-1.2.4-2.6.8

x86_64
libgsttag-1_0-0-1.2.4-2.6.8
libgstrtp-1_0-0-1.2.4-2.6.8
libgstapp-1_0-0-32bit-1.2.4-2.6.8
libgstallocators-1_0-0-1.2.4-2.6.8
gstreamer-plugins-base-1.2.4-2.6.8
libgstallocators-1_0-0-debuginfo-1.2.4-2.6.8
libgstrtsp-1_0-0-debuginfo-1.2.4-2.6.8
libgstpbutils-1_0-0-32bit-1.2.4-2.6.8
libgstrtp-1_0-0-debuginfo-1.2.4-2.6.8
libgstapp-1_0-0-debuginfo-32bit-1.2.4-2.6.8
gstreamer-plugins-base-debuginfo-32bit-1.2.4-2.6.8
libgstpbutils-1_0-0-debuginfo-1.2.4-2.6.8
libgsttag-1_0-0-32bit-1.2.4-2.6.8
libgstapp-1_0-0-debuginfo-1.2.4-2.6.8
libgstfft-1_0-0-1.2.4-2.6.8
libgsttag-1_0-0-debuginfo-32bit-1.2.4-2.6.8
gstreamer-plugins-base-debuginfo-1.2.4-2.6.8
libgstsdp-1_0-0-debuginfo-1.2.4-2.6.8
libgstriff-1_0-0-debuginfo-1.2.4-2.6.8
libgstrtsp-1_0-0-1.2.4-2.6.8
libgstaudio-1_0-0-debuginfo-1.2.4-2.6.8
libgstpbutils-1_0-0-1.2.4-2.6.8
libgstaudio-1_0-0-32bit-1.2.4-2.6.8
libgsttag-1_0-0-debuginfo-1.2.4-2.6.8
libgstfft-1_0-0-debuginfo-1.2.4-2.6.8
libgstpbutils-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstvideo-1_0-0-debuginfo-1.2.4-2.6.8
libgstvideo-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstapp-1_0-0-1.2.4-2.6.8
libgstvideo-1_0-0-32bit-1.2.4-2.6.8
libgstaudio-1_0-0-1.2.4-2.6.8
libgstriff-1_0-0-1.2.4-2.6.8
libgstaudio-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstsdp-1_0-0-1.2.4-2.6.8
libgstvideo-1_0-0-1.2.4-2.6.8
gstreamer-plugins-base-debugsource-1.2.4-2.6.8

SuSE SLED 12 SP1
x86_64
libgsttag-1_0-0-1.2.4-2.6.8
libgstrtp-1_0-0-1.2.4-2.6.8
libgstfft-1_0-0-1.2.4-2.6.8
gstreamer-plugins-base-1.2.4-2.6.8
libgstaudio-1_0-0-32bit-1.2.4-2.6.8
libgstallocators-1_0-0-debuginfo-1.2.4-2.6.8
libgstrtsp-1_0-0-debuginfo-1.2.4-2.6.8
libgstsdp-1_0-0-debuginfo-1.2.4-2.6.8
gstreamer-plugins-base-debuginfo-32bit-1.2.4-2.6.8
libgstrtp-1_0-0-debuginfo-1.2.4-2.6.8

libgstfft-1_0-0-32bit-1.2.4-2.6.8
libgstapp-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstapp-1_0-0-32bit-1.2.4-2.6.8
typelib-1_0-GstPbutils-1_0-1.2.4-2.6.8
typelib-1_0-GstAudio-1_0-1.2.4-2.6.8
libgstpbutils-1_0-0-debuginfo-1.2.4-2.6.8
libgsttag-1_0-0-32bit-1.2.4-2.6.8
libgstapp-1_0-0-debuginfo-1.2.4-2.6.8
libgsttag-1_0-0-debuginfo-32bit-1.2.4-2.6.8
typelib-1_0-GstVideo-1_0-1.2.4-2.6.8
gstreamer-plugins-base-debuginfo-1.2.4-2.6.8
libgstallocators-1_0-0-1.2.4-2.6.8
libgstpbutils-1_0-0-32bit-1.2.4-2.6.8
typelib-1_0-GstTag-1_0-1.2.4-2.6.8
libgstrtsp-1_0-0-1.2.4-2.6.8
libgstaudio-1_0-0-debuginfo-1.2.4-2.6.8
libgstpbutils-1_0-0-1.2.4-2.6.8
libgstfft-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgsttag-1_0-0-debuginfo-1.2.4-2.6.8
libgstfft-1_0-0-debuginfo-1.2.4-2.6.8
libgstpbutils-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstvideo-1_0-0-debuginfo-1.2.4-2.6.8
libgstvideo-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstriff-1_0-0-debuginfo-1.2.4-2.6.8
libgstapp-1_0-0-1.2.4-2.6.8
libgstvideo-1_0-0-32bit-1.2.4-2.6.8
libgstaudio-1_0-0-1.2.4-2.6.8
libgstriff-1_0-0-1.2.4-2.6.8
libgstaudio-1_0-0-debuginfo-32bit-1.2.4-2.6.8
libgstsdp-1_0-0-1.2.4-2.6.8
libgstvideo-1_0-0-1.2.4-2.6.8
gstreamer-plugins-base-debugsource-1.2.4-2.6.8

noarch
gstreamer-plugins-base-lang-1.2.4-2.6.8

145312 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1039-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5839, CVE-2017-5842, CVE-2017-5844

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1039-1

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-April/002805.html

SuSE SLED 12 SP2
x86_64
libgstvideo-1_0-0-debuginfo-1.8.3-12.11
libgstrtsp-1_0-0-1.8.3-12.11
libgstfft-1_0-0-32bit-1.8.3-12.11
libgstpbutils-1_0-0-debuginfo-32bit-1.8.3-12.11

libgstvideo-1_0-0-32bit-1.8.3-12.11
libgstvideo-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstsdp-1_0-0-debuginfo-1.8.3-12.11
libgstrtp-1_0-0-1.8.3-12.11
typelib-1_0-GstPbutils-1_0-1.8.3-12.11
libgstfft-1_0-0-1.8.3-12.11
libgstaudio-1_0-0-32bit-1.8.3-12.11
gstreamer-plugins-base-debugsource-1.8.3-12.11
libgstapp-1_0-0-32bit-1.8.3-12.11
libgstsdp-1_0-0-1.8.3-12.11
libgstriff-1_0-0-1.8.3-12.11
libgsttag-1_0-0-32bit-1.8.3-12.11
gstreamer-plugins-base-debuginfo-32bit-1.8.3-12.11
libgstrtsp-1_0-0-debuginfo-1.8.3-12.11
libgstallocators-1_0-0-1.8.3-12.11
libgstriff-1_0-0-debuginfo-1.8.3-12.11
libgstpbutils-1_0-0-debuginfo-1.8.3-12.11
libgstrtp-1_0-0-debuginfo-1.8.3-12.11
libgstfft-1_0-0-debuginfo-1.8.3-12.11
gstreamer-plugins-base-debuginfo-1.8.3-12.11
libgstapp-1_0-0-debuginfo-1.8.3-12.11
libgsttag-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstaudio-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstapp-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstaudio-1_0-0-1.8.3-12.11
libgstapp-1_0-0-1.8.3-12.11
libgstallocators-1_0-0-debuginfo-1.8.3-12.11
libgstaudio-1_0-0-debuginfo-1.8.3-12.11
gstreamer-plugins-base-1.8.3-12.11
typelib-1_0-GstAudio-1_0-1.8.3-12.11
typelib-1_0-GstVideo-1_0-1.8.3-12.11
libgstfft-1_0-0-debuginfo-32bit-1.8.3-12.11
typelib-1_0-GstTag-1_0-1.8.3-12.11
libgsttag-1_0-0-debuginfo-1.8.3-12.11
libgstvideo-1_0-0-1.8.3-12.11
libgsttag-1_0-0-1.8.3-12.11
libgstpbutils-1_0-0-32bit-1.8.3-12.11
libgstpbutils-1_0-0-1.8.3-12.11

noarch
gstreamer-plugins-base-lang-1.8.3-12.11

SuSE SLES 12 SP2
noarch
gstreamer-plugins-base-lang-1.8.3-12.11

x86_64
libgstaudio-1_0-0-32bit-1.8.3-12.11
libgstpbutils-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstvideo-1_0-0-32bit-1.8.3-12.11
libgstvideo-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstsdp-1_0-0-debuginfo-1.8.3-12.11
libgstrtp-1_0-0-1.8.3-12.11
libgstfft-1_0-0-1.8.3-12.11
libgstvideo-1_0-0-debuginfo-1.8.3-12.11
gstreamer-plugins-base-debugsource-1.8.3-12.11
libgstapp-1_0-0-32bit-1.8.3-12.11
libgstsdp-1_0-0-1.8.3-12.11
libgstriff-1_0-0-1.8.3-12.11
libgsttag-1_0-0-32bit-1.8.3-12.11

gstreamer-plugins-base-debuginfo-32bit-1.8.3-12.11
libgstrtsp-1_0-0-debuginfo-1.8.3-12.11
libgstallocators-1_0-0-1.8.3-12.11
libgstriff-1_0-0-debuginfo-1.8.3-12.11
libgstpbutils-1_0-0-debuginfo-1.8.3-12.11
libgsttag-1_0-0-1.8.3-12.11
libgstfft-1_0-0-debuginfo-1.8.3-12.11
libgstpbutils-1_0-0-32bit-1.8.3-12.11
gstreamer-plugins-base-debuginfo-1.8.3-12.11
libgsttag-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstaudio-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstapp-1_0-0-debuginfo-32bit-1.8.3-12.11
libgstaudio-1_0-0-1.8.3-12.11
libgstapp-1_0-0-1.8.3-12.11
gstreamer-plugins-base-1.8.3-12.11
libgstallocators-1_0-0-debuginfo-1.8.3-12.11
libgstaudio-1_0-0-debuginfo-1.8.3-12.11
libgstrtp-1_0-0-debuginfo-1.8.3-12.11
libgsttag-1_0-0-debuginfo-1.8.3-12.11
libgstrtsp-1_0-0-1.8.3-12.11
libgstvideo-1_0-0-1.8.3-12.11
libgstapp-1_0-0-debuginfo-1.8.3-12.11
libgstpbutils-1_0-0-1.8.3-12.11

160232 - CentOS 7 CESA-2017-0907 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
CESA-2017-0907

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-April/022376.html

CentOS 7
x86_64
libuuid-2.23.2-33.el7_3.2
libuuid-devel-2.23.2-33.el7_3.2
libblkid-devel-2.23.2-33.el7_3.2
libblkid-2.23.2-33.el7_3.2
libmount-2.23.2-33.el7_3.2
libmount-devel-2.23.2-33.el7_3.2
util-linux-2.23.2-33.el7_3.2
uuidd-2.23.2-33.el7_3.2

i686
libuuid-2.23.2-33.el7_3.2
libuuid-devel-2.23.2-33.el7_3.2
libblkid-devel-2.23.2-33.el7_3.2
libblkid-2.23.2-33.el7_3.2
libmount-2.23.2-33.el7_3.2
libmount-devel-2.23.2-33.el7_3.2

util-linux-2.23.2-33.el7_3.2

160235 - CentOS 7 CESA-2017-0914 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
CESA-2017-0914

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-April/022359.html

CentOS 7
x86_64
libreoffice-graphicfilter-5.0.6.2-5.el7_3.1
libreoffice-langpack-gl-5.0.6.2-5.el7_3.1
libreoffice-langpack-it-5.0.6.2-5.el7_3.1
libreoffice-langpack-ga-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hant-5.0.6.2-5.el7_3.1
libreoffice-langpack-xh-5.0.6.2-5.el7_3.1
libreoffice-langpack-ca-5.0.6.2-5.el7_3.1
libreoffice-langpack-lt-5.0.6.2-5.el7_3.1
libreoffice-langpack-da-5.0.6.2-5.el7_3.1
libreoffice-langpack-de-5.0.6.2-5.el7_3.1
libreoffice-langpack-fi-5.0.6.2-5.el7_3.1
libreoffice-ogltrans-5.0.6.2-5.el7_3.1
libreoffice-langpack-gu-5.0.6.2-5.el7_3.1
libreoffice-base-5.0.6.2-5.el7_3.1
libreoffice-langpack-kk-5.0.6.2-5.el7_3.1
libreoffice-langpack-th-5.0.6.2-5.el7_3.1
libreoffice-ure-5.0.6.2-5.el7_3.1
libreoffice-langpack-nr-5.0.6.2-5.el7_3.1
libreoffice-calc-5.0.6.2-5.el7_3.1
libreoffice-sdk-doc-5.0.6.2-5.el7_3.1
libreoffice-langpack-nl-5.0.6.2-5.el7_3.1
libreoffice-langpack-pt-PT-5.0.6.2-5.el7_3.1
libreoffice-langpack-el-5.0.6.2-5.el7_3.1
libreoffice-langpack-si-5.0.6.2-5.el7_3.1
libreoffice-rhino-5.0.6.2-5.el7_3.1
libreoffice-langpack-ru-5.0.6.2-5.el7_3.1
libreoffice-5.0.6.2-5.el7_3.1
libreoffice-langpack-bn-5.0.6.2-5.el7_3.1
libreoffice-langpack-ja-5.0.6.2-5.el7_3.1
libreoffice-langpack-nso-5.0.6.2-5.el7_3.1
libreoffice-langpack-hi-5.0.6.2-5.el7_3.1
libreoffice-langpack-nb-5.0.6.2-5.el7_3.1
libreoffice-langpack-kn-5.0.6.2-5.el7_3.1
libreoffice-langpack-cy-5.0.6.2-5.el7_3.1
libreoffice-langpack-zu-5.0.6.2-5.el7_3.1
libreoffice-langpack-ro-5.0.6.2-5.el7_3.1
libreoffice-wiki-publisher-5.0.6.2-5.el7_3.1
libreoffice-gdb-debug-support-5.0.6.2-5.el7_3.1

libreoffice-langpack-uk-5.0.6.2-5.el7_3.1
libreoffice-langpack-sk-5.0.6.2-5.el7_3.1
libreoffice-langpack-tr-5.0.6.2-5.el7_3.1
libreoffice-langpack-ta-5.0.6.2-5.el7_3.1
libreoffice-langpack-dz-5.0.6.2-5.el7_3.1
libreoffice-langpack-sl-5.0.6.2-5.el7_3.1
libreoffice-langpack-st-5.0.6.2-5.el7_3.1
libreoffice-langpack-fa-5.0.6.2-5.el7_3.1
libreoffice-writer-5.0.6.2-5.el7_3.1
libreoffice-postgresql-5.0.6.2-5.el7_3.1
libreoffice-langpack-ss-5.0.6.2-5.el7_3.1
libreoffice-langpack-eu-5.0.6.2-5.el7_3.1
libreoffice-langpack-ar-5.0.6.2-5.el7_3.1
libreoffice-langpack-or-5.0.6.2-5.el7_3.1
libreoffice-pyuno-5.0.6.2-5.el7_3.1
libreoffice-langpack-pl-5.0.6.2-5.el7_3.1
libreoffice-langpack-te-5.0.6.2-5.el7_3.1
libreoffice-langpack-pa-5.0.6.2-5.el7_3.1
libreoffice-xsltfilter-5.0.6.2-5.el7_3.1
libreoffice-langpack-mr-5.0.6.2-5.el7_3.1
libreoffice-sdk-5.0.6.2-5.el7_3.1
libreoffice-draw-5.0.6.2-5.el7_3.1
libreoffice-librelogo-5.0.6.2-5.el7_3.1
libreoffice-langpack-mai-5.0.6.2-5.el7_3.1
libreoffice-langpack-ml-5.0.6.2-5.el7_3.1
libreoffice-langpack-hu-5.0.6.2-5.el7_3.1
libreoffice-core-5.0.6.2-5.el7_3.1
libreoffice-langpack-sr-5.0.6.2-5.el7_3.1
libreoffice-emailmerge-5.0.6.2-5.el7_3.1
libreoffice-langpack-sv-5.0.6.2-5.el7_3.1
libreoffice-langpack-af-5.0.6.2-5.el7_3.1
libreoffice-langpack-es-5.0.6.2-5.el7_3.1
libreoffice-langpack-cs-5.0.6.2-5.el7_3.1
libreoffice-langpack-tn-5.0.6.2-5.el7_3.1
libreoffice-langpack-ve-5.0.6.2-5.el7_3.1
libreoffice-filters-5.0.6.2-5.el7_3.1
libreoffice-langpack-he-5.0.6.2-5.el7_3.1
libreoffice-langpack-et-5.0.6.2-5.el7_3.1
libreoffice-nlpsolver-5.0.6.2-5.el7_3.1
libreoffice-bsh-5.0.6.2-5.el7_3.1
libreoffice-langpack-nn-5.0.6.2-5.el7_3.1
libreoffice-langpack-bg-5.0.6.2-5.el7_3.1
libreoffice-langpack-en-5.0.6.2-5.el7_3.1
libreoffice-langpack-ts-5.0.6.2-5.el7_3.1
libreoffice-langpack-pt-BR-5.0.6.2-5.el7_3.1
libreoffice-langpack-lv-5.0.6.2-5.el7_3.1
libreoffice-langpack-hr-5.0.6.2-5.el7_3.1
libreoffice-glade-5.0.6.2-5.el7_3.1
libreoffice-officebean-5.0.6.2-5.el7_3.1
libreoffice-impress-5.0.6.2-5.el7_3.1
libreoffice-langpack-fr-5.0.6.2-5.el7_3.1
libreoffice-math-5.0.6.2-5.el7_3.1
libreoffice-pdfimport-5.0.6.2-5.el7_3.1
libreoffice-langpack-ko-5.0.6.2-5.el7_3.1
libreoffice-langpack-br-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hans-5.0.6.2-5.el7_3.1
libreoffice-langpack-as-5.0.6.2-5.el7_3.1

noarch
autocorr-ja-5.0.6.2-5.el7_3.1

autocorr-cs-5.0.6.2-5.el7_3.1
autocorr-it-5.0.6.2-5.el7_3.1
autocorr-hr-5.0.6.2-5.el7_3.1
autocorr-fa-5.0.6.2-5.el7_3.1
autocorr-ro-5.0.6.2-5.el7_3.1
autocorr-fi-5.0.6.2-5.el7_3.1
autocorr-pl-5.0.6.2-5.el7_3.1
autocorr-vi-5.0.6.2-5.el7_3.1
autocorr-zh-5.0.6.2-5.el7_3.1
autocorr-lb-5.0.6.2-5.el7_3.1
autocorr-sv-5.0.6.2-5.el7_3.1
autocorr-sr-5.0.6.2-5.el7_3.1
autocorr-en-5.0.6.2-5.el7_3.1
autocorr-mn-5.0.6.2-5.el7_3.1
autocorr-hu-5.0.6.2-5.el7_3.1
autocorr-ga-5.0.6.2-5.el7_3.1
autocorr-tr-5.0.6.2-5.el7_3.1
autocorr-de-5.0.6.2-5.el7_3.1
libreoffice-opensymbol-fonts-5.0.6.2-5.el7_3.1
autocorr-sk-5.0.6.2-5.el7_3.1
autocorr-fr-5.0.6.2-5.el7_3.1
autocorr-nl-5.0.6.2-5.el7_3.1
autocorr-is-5.0.6.2-5.el7_3.1
autocorr-da-5.0.6.2-5.el7_3.1
autocorr-af-5.0.6.2-5.el7_3.1
autocorr-ko-5.0.6.2-5.el7_3.1
autocorr-bg-5.0.6.2-5.el7_3.1
autocorr-sl-5.0.6.2-5.el7_3.1
autocorr-es-5.0.6.2-5.el7_3.1
autocorr-pt-5.0.6.2-5.el7_3.1
autocorr-ca-5.0.6.2-5.el7_3.1
autocorr-ru-5.0.6.2-5.el7_3.1
autocorr-lt-5.0.6.2-5.el7_3.1

160238 - CentOS 7 CESA-2017-0906 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
CESA-2017-0906

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-April/022380.html

CentOS 7
x86_64
httpd-2.4.6-45.el7.centos.4
mod_ssl-2.4.6-45.el7.centos.4
mod_proxy_html-2.4.6-45.el7.centos.4
httpd-devel-2.4.6-45.el7.centos.4
mod_ldap-2.4.6-45.el7.centos.4
mod_session-2.4.6-45.el7.centos.4

httpd-tools-2.4.6-45.el7.centos.4

noarch
httpd-manual-2.4.6-45.el7.centos.4

163324 - Oracle Enterprise Linux ELSA-2017-0906 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
ELSA-2017-0906

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006839.html

OEL7
x86_64
httpd-devel-2.4.6-45.0.1.el7_3.4
httpd-manual-2.4.6-45.0.1.el7_3.4
httpd-2.4.6-45.0.1.el7_3.4
httpd-tools-2.4.6-45.0.1.el7_3.4
mod_ssl-2.4.6-45.0.1.el7_3.4
mod_session-2.4.6-45.0.1.el7_3.4
mod_ldap-2.4.6-45.0.1.el7_3.4
mod_proxy_html-2.4.6-45.0.1.el7_3.4

163327 - Oracle Enterprise Linux ELSA-2017-0907 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
ELSA-2017-0907

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006840.html

OEL7
x86_64
libmount-devel-2.23.2-33.0.1.el7_3.2
uuidd-2.23.2-33.0.1.el7_3.2
libblkid-2.23.2-33.0.1.el7_3.2
libuuid-devel-2.23.2-33.0.1.el7_3.2
libuuid-2.23.2-33.0.1.el7_3.2
libmount-2.23.2-33.0.1.el7_3.2

util-linux-2.23.2-33.0.1.el7_3.2
libblkid-devel-2.23.2-33.0.1.el7_3.2

163330 - Oracle Enterprise Linux ELSA-2017-0979 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
ELSA-2017-0979

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006869.html

OEL6
x86_64
libreoffice-langpack-ur-4.3.7.2-2.0.1.el6_9.1
libreoffice-pyuno-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-hr-4.3.7.2-2.0.1.el6_9.1
libreoffice-sdk-4.3.7.2-2.0.1.el6_9.1
autocorr-sl-4.3.7.2-2.0.1.el6_9.1
autocorr-bg-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-tr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nr-4.3.7.2-2.0.1.el6_9.1
autocorr-es-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.0.1.el6_9.1
libreoffice-pdfimport-4.3.7.2-2.0.1.el6_9.1
autocorr-ru-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.0.1.el6_9.1
autocorr-is-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.0.1.el6_9.1
autocorr-en-4.3.7.2-2.0.1.el6_9.1
autocorr-sk-4.3.7.2-2.0.1.el6_9.1
libreoffice-writer-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-gl-4.3.7.2-2.0.1.el6_9.1
autocorr-fi-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.0.1.el6_9.1
libreoffice-sdk-doc-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.0.1.el6_9.1
libreoffice-glade-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-zh-Hans-4.3.7.2-2.0.1.el6_9.1
autocorr-fa-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.0.1.el6_9.1
libreoffice-ure-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-pl-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ve-4.3.7.2-2.0.1.el6_9.1

autocorr-tr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-pt-PT-4.3.7.2-2.0.1.el6_9.1
autocorr-ko-4.3.7.2-2.0.1.el6_9.1
autocorr-ro-4.3.7.2-2.0.1.el6_9.1
libreoffice-rhino-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.0.1.el6_9.1
autocorr-pt-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-mr-4.3.7.2-2.0.1.el6_9.1
libreoffice-emailmerge-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.0.1.el6_9.1
autocorr-da-4.3.7.2-2.0.1.el6_9.1
autocorr-de-4.3.7.2-2.0.1.el6_9.1
libreoffice-headless-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.0.1.el6_9.1
autocorr-zh-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-th-4.3.7.2-2.0.1.el6_9.1
autocorr-ja-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-mai-4.3.7.2-2.0.1.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.0.1.el6_9.1
libreoffice-4.3.7.2-2.0.1.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.0.1.el6_9.1
libreoffice-librelogo-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ar-4.3.7.2-2.0.1.el6_9.1
autocorr-cs-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-pa-4.3.7.2-2.0.1.el6_9.1
libreoffice-core-4.3.7.2-2.0.1.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.0.1.el6_9.1
autocorr-ga-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-sr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-el-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-tn-4.3.7.2-2.0.1.el6_9.1
libreoffice-bsh-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-eu-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.0.1.el6_9.1
libreoffice-nlpsolver-4.3.7.2-2.0.1.el6_9.1
libreoffice-math-4.3.7.2-2.0.1.el6_9.1
libreoffice-ogltrans-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-cy-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-en-4.3.7.2-2.0.1.el6_9.1
libreoffice-impress-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.0.1.el6_9.1
autocorr-hr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-kn-4.3.7.2-2.0.1.el6_9.1
autocorr-ca-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nl-4.3.7.2-2.0.1.el6_9.1
libreoffice-filters-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-te-4.3.7.2-2.0.1.el6_9.1
libreoffice-draw-4.3.7.2-2.0.1.el6_9.1
autocorr-lt-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ta-4.3.7.2-2.0.1.el6_9.1
autocorr-vi-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.0.1.el6_9.1
autocorr-lb-4.3.7.2-2.0.1.el6_9.1

libreoffice-langpack-hu-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.0.1.el6_9.1
autocorr-sr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ko-4.3.7.2-2.0.1.el6_9.1
autocorr-it-4.3.7.2-2.0.1.el6_9.1
autocorr-af-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.0.1.el6_9.1
libreoffice-officebean-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.0.1.el6_9.1
libreoffice-calc-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.0.1.el6_9.1
libreoffice-base-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-fi-4.3.7.2-2.0.1.el6_9.1
autocorr-pl-4.3.7.2-2.0.1.el6_9.1
libreoffice-wiki-publisher-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-de-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.0.1.el6_9.1
autocorr-nl-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-or-4.3.7.2-2.0.1.el6_9.1
autocorr-fr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.0.1.el6_9.1
autocorr-hu-4.3.7.2-2.0.1.el6_9.1
libreoffice-opensymbol-fonts-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.0.1.el6_9.1
autocorr-sv-4.3.7.2-2.0.1.el6_9.1
autocorr-mn-4.3.7.2-2.0.1.el6_9.1

i386
libreoffice-langpack-ur-4.3.7.2-2.0.1.el6_9.1
libreoffice-pyuno-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-hr-4.3.7.2-2.0.1.el6_9.1
libreoffice-sdk-4.3.7.2-2.0.1.el6_9.1
autocorr-sl-4.3.7.2-2.0.1.el6_9.1
autocorr-bg-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-tr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nr-4.3.7.2-2.0.1.el6_9.1
autocorr-es-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.0.1.el6_9.1
libreoffice-pdfimport-4.3.7.2-2.0.1.el6_9.1
autocorr-ru-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.0.1.el6_9.1
autocorr-is-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.0.1.el6_9.1
autocorr-en-4.3.7.2-2.0.1.el6_9.1
autocorr-sk-4.3.7.2-2.0.1.el6_9.1
libreoffice-writer-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-gl-4.3.7.2-2.0.1.el6_9.1
autocorr-fi-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.0.1.el6_9.1
libreoffice-sdk-doc-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.0.1.el6_9.1
libreoffice-glade-4.3.7.2-2.0.1.el6_9.1

libreoffice-langpack-zh-Hans-4.3.7.2-2.0.1.el6_9.1
autocorr-fa-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.0.1.el6_9.1
libreoffice-ure-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.0.1.el6_9.1
libreoffice-langpack-pl-4.3.7.2-2.0.1.el6_9.1

175153 - Scientific Linux Security ERRATA Moderate: httpd on SL7.x x86_64 (1704-7439)

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: httpd on SL7.x x86_64 (1704-7439)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=7439

SL7
x86_64
mod_ldap-2.4.6-45.el7_3.4
httpd-debuginfo-2.4.6-45.el7_3.4
mod_session-2.4.6-45.el7_3.4
mod_proxy_html-2.4.6-45.el7_3.4
httpd-2.4.6-45.el7_3.4
httpd-tools-2.4.6-45.el7_3.4
httpd-devel-2.4.6-45.el7_3.4
mod_ssl-2.4.6-45.el7_3.4

noarch
httpd-manual-2.4.6-45.el7_3.4

175155 - Scientific Linux Security ERRATA Moderate: libreoffice on SL7.x x86_64 (1704-7807)

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreoffice on SL7.x x86_64 (1704-7807)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=7807

SL7
x86_64

libreoffice-graphicfilter-5.0.6.2-5.el7_3.1
libreoffice-debuginfo-5.0.6.2-5.el7_3.1
libreoffice-langpack-gl-5.0.6.2-5.el7_3.1
libreoffice-langpack-it-5.0.6.2-5.el7_3.1
libreoffice-langpack-ga-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hant-5.0.6.2-5.el7_3.1
libreoffice-langpack-xh-5.0.6.2-5.el7_3.1
libreoffice-langpack-ca-5.0.6.2-5.el7_3.1
libreoffice-langpack-lt-5.0.6.2-5.el7_3.1
libreoffice-langpack-ss-5.0.6.2-5.el7_3.1
libreoffice-langpack-zu-5.0.6.2-5.el7_3.1
libreoffice-langpack-st-5.0.6.2-5.el7_3.1
libreoffice-langpack-fi-5.0.6.2-5.el7_3.1
libreoffice-ogltrans-5.0.6.2-5.el7_3.1
libreoffice-langpack-gu-5.0.6.2-5.el7_3.1
libreoffice-base-5.0.6.2-5.el7_3.1
libreoffice-langpack-kk-5.0.6.2-5.el7_3.1
libreoffice-langpack-th-5.0.6.2-5.el7_3.1
libreoffice-ure-5.0.6.2-5.el7_3.1
libreoffice-langpack-eu-5.0.6.2-5.el7_3.1
libreoffice-calc-5.0.6.2-5.el7_3.1
libreoffice-sdk-doc-5.0.6.2-5.el7_3.1
libreoffice-langpack-nl-5.0.6.2-5.el7_3.1
libreoffice-langpack-pt-PT-5.0.6.2-5.el7_3.1
libreoffice-langpack-el-5.0.6.2-5.el7_3.1
libreoffice-langpack-si-5.0.6.2-5.el7_3.1
libreoffice-rhino-5.0.6.2-5.el7_3.1
libreoffice-langpack-ru-5.0.6.2-5.el7_3.1
libreoffice-5.0.6.2-5.el7_3.1
libreoffice-langpack-bn-5.0.6.2-5.el7_3.1
libreoffice-langpack-ja-5.0.6.2-5.el7_3.1
libreoffice-langpack-nso-5.0.6.2-5.el7_3.1
libreoffice-langpack-hi-5.0.6.2-5.el7_3.1
libreoffice-langpack-nb-5.0.6.2-5.el7_3.1
libreoffice-langpack-kn-5.0.6.2-5.el7_3.1
libreoffice-langpack-cy-5.0.6.2-5.el7_3.1
libreoffice-langpack-es-5.0.6.2-5.el7_3.1
libreoffice-langpack-nr-5.0.6.2-5.el7_3.1
libreoffice-langpack-ro-5.0.6.2-5.el7_3.1
libreoffice-wiki-publisher-5.0.6.2-5.el7_3.1
libreoffice-gdb-debug-support-5.0.6.2-5.el7_3.1
libreoffice-langpack-uk-5.0.6.2-5.el7_3.1
libreoffice-langpack-sk-5.0.6.2-5.el7_3.1
libreoffice-langpack-tr-5.0.6.2-5.el7_3.1
libreoffice-langpack-ta-5.0.6.2-5.el7_3.1
libreoffice-langpack-dz-5.0.6.2-5.el7_3.1
libreoffice-langpack-sl-5.0.6.2-5.el7_3.1
libreoffice-langpack-fa-5.0.6.2-5.el7_3.1
libreoffice-writer-5.0.6.2-5.el7_3.1
libreoffice-postgresql-5.0.6.2-5.el7_3.1
libreoffice-langpack-ar-5.0.6.2-5.el7_3.1
libreoffice-langpack-or-5.0.6.2-5.el7_3.1
libreoffice-pyuno-5.0.6.2-5.el7_3.1
libreoffice-langpack-pl-5.0.6.2-5.el7_3.1
libreoffice-langpack-te-5.0.6.2-5.el7_3.1
libreoffice-langpack-pa-5.0.6.2-5.el7_3.1
libreoffice-xsltfilter-5.0.6.2-5.el7_3.1
libreoffice-langpack-mr-5.0.6.2-5.el7_3.1
libreoffice-sdk-5.0.6.2-5.el7_3.1
libreoffice-draw-5.0.6.2-5.el7_3.1

libreoffice-librelogo-5.0.6.2-5.el7_3.1
libreoffice-langpack-mai-5.0.6.2-5.el7_3.1
libreoffice-langpack-ml-5.0.6.2-5.el7_3.1
libreoffice-langpack-hu-5.0.6.2-5.el7_3.1
libreoffice-core-5.0.6.2-5.el7_3.1
libreoffice-langpack-sr-5.0.6.2-5.el7_3.1
libreoffice-emailmerge-5.0.6.2-5.el7_3.1
libreoffice-langpack-da-5.0.6.2-5.el7_3.1
libreoffice-langpack-sv-5.0.6.2-5.el7_3.1
libreoffice-langpack-af-5.0.6.2-5.el7_3.1
libreoffice-langpack-de-5.0.6.2-5.el7_3.1
libreoffice-langpack-cs-5.0.6.2-5.el7_3.1
libreoffice-langpack-tn-5.0.6.2-5.el7_3.1
libreoffice-langpack-ve-5.0.6.2-5.el7_3.1
libreoffice-filters-5.0.6.2-5.el7_3.1
libreoffice-langpack-he-5.0.6.2-5.el7_3.1
libreoffice-langpack-et-5.0.6.2-5.el7_3.1
libreoffice-nlpsolver-5.0.6.2-5.el7_3.1
libreoffice-bsh-5.0.6.2-5.el7_3.1
libreoffice-langpack-nn-5.0.6.2-5.el7_3.1
libreoffice-langpack-bg-5.0.6.2-5.el7_3.1
libreoffice-langpack-en-5.0.6.2-5.el7_3.1
libreoffice-langpack-ts-5.0.6.2-5.el7_3.1
libreoffice-langpack-pt-BR-5.0.6.2-5.el7_3.1
libreoffice-langpack-lv-5.0.6.2-5.el7_3.1
libreoffice-langpack-hr-5.0.6.2-5.el7_3.1
libreoffice-glade-5.0.6.2-5.el7_3.1
libreoffice-officebean-5.0.6.2-5.el7_3.1
libreoffice-impress-5.0.6.2-5.el7_3.1
libreoffice-langpack-fr-5.0.6.2-5.el7_3.1
libreoffice-math-5.0.6.2-5.el7_3.1
libreoffice-pdfimport-5.0.6.2-5.el7_3.1
libreoffice-langpack-ko-5.0.6.2-5.el7_3.1
libreoffice-langpack-br-5.0.6.2-5.el7_3.1
libreoffice-langpack-zh-Hans-5.0.6.2-5.el7_3.1
libreoffice-langpack-as-5.0.6.2-5.el7_3.1

noarch
autocorr-ja-5.0.6.2-5.el7_3.1
autocorr-cs-5.0.6.2-5.el7_3.1
autocorr-it-5.0.6.2-5.el7_3.1
autocorr-hr-5.0.6.2-5.el7_3.1
autocorr-fa-5.0.6.2-5.el7_3.1
autocorr-ro-5.0.6.2-5.el7_3.1
autocorr-fi-5.0.6.2-5.el7_3.1
autocorr-pl-5.0.6.2-5.el7_3.1
autocorr-vi-5.0.6.2-5.el7_3.1
autocorr-zh-5.0.6.2-5.el7_3.1
autocorr-lb-5.0.6.2-5.el7_3.1
autocorr-sv-5.0.6.2-5.el7_3.1
autocorr-sr-5.0.6.2-5.el7_3.1
autocorr-en-5.0.6.2-5.el7_3.1
autocorr-mn-5.0.6.2-5.el7_3.1
autocorr-hu-5.0.6.2-5.el7_3.1
autocorr-ga-5.0.6.2-5.el7_3.1
autocorr-tr-5.0.6.2-5.el7_3.1
autocorr-de-5.0.6.2-5.el7_3.1
libreoffice-opensymbol-fonts-5.0.6.2-5.el7_3.1
autocorr-sk-5.0.6.2-5.el7_3.1
autocorr-fr-5.0.6.2-5.el7_3.1

autocorr-nl-5.0.6.2-5.el7_3.1
autocorr-is-5.0.6.2-5.el7_3.1
autocorr-da-5.0.6.2-5.el7_3.1
autocorr-af-5.0.6.2-5.el7_3.1
autocorr-ko-5.0.6.2-5.el7_3.1
autocorr-bg-5.0.6.2-5.el7_3.1
autocorr-sl-5.0.6.2-5.el7_3.1
autocorr-es-5.0.6.2-5.el7_3.1
autocorr-pt-5.0.6.2-5.el7_3.1
autocorr-ca-5.0.6.2-5.el7_3.1
autocorr-ru-5.0.6.2-5.el7_3.1
autocorr-lt-5.0.6.2-5.el7_3.1

175157 - Scientific Linux Security ERRATA Moderate: util-linux on SL7.x x86_64 (1704-7095)

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: util-linux on SL7.x x86_64 (1704-7095)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=7095

SL7
x86_64
libuuid-2.23.2-33.el7_3.2
libblkid-devel-2.23.2-33.el7_3.2
libuuid-devel-2.23.2-33.el7_3.2
libblkid-2.23.2-33.el7_3.2
libmount-2.23.2-33.el7_3.2
uuidd-2.23.2-33.el7_3.2
util-linux-2.23.2-33.el7_3.2
libmount-devel-2.23.2-33.el7_3.2
util-linux-debuginfo-2.23.2-33.el7_3.2

191942 - Fedora Linux 24 FEDORA-2017-66fd940572 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
FEDORA-2017-66fd940572

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/2017/4/?count=200&page=3

Fedora Core 24

libpng15-1.5.28-1.fc24

191962 - Fedora Linux 25 FEDORA-2017-cf1944f480 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
FEDORA-2017-cf1944f480

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/2017/4/?count=200&page=3

Fedora Core 25

libpng15-1.5.28-1.fc25

191967 - Fedora Linux 25 FEDORA-2017-bad9942e42 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bad9942e42

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/2017/4/?count=200&page=2

Fedora Core 25

libpng12-1.2.57-1.fc25

191969 - Fedora Linux 24 FEDORA-2017-84bc8ac268 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
FEDORA-2017-84bc8ac268

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/2017/4/?count=200&page=2

Fedora Core 24

libpng12-1.2.57-1.fc24

21665 - Dell iDRAC Cross-Site-Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-7275

Description

A cross-site-scripting vulnerability is present in some versions of Dell Integrated Dell Remote Access Controller (iDRAC).

Observation

Dell Integrated Dell Remote Access Controller is a popular embedded server management solution.

A cross-site-scripting vulnerability is present in some versions of Dell Integrated Dell Remote Access Controller (iDRAC). The flaw lies in an unknown component of Dell Integrated Dell Remote Access Controller. Successful exploitation could allow an attacker to execute arbitrary code on vulnerable installations.

130742 - Debian Linux 8.0 DSA-3829-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-6644

Description

The scan detected that the host is missing the following update:
DSA-3829-1

Observation

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

http://www.debian.org/security/2017/dsa-3829

Debian 8.0
all
libbcmail-java_1.49+dfsg-3+deb8u2
libbcpkix-java_1.49+dfsg-3+deb8u2
libbcpkix-java-doc_1.49+dfsg-3+deb8u2
libbcpg-java_1.49+dfsg-3+deb8u2
libbcmail-java-doc_1.49+dfsg-3+deb8u2
libbcprov-java-doc_1.49+dfsg-3+deb8u2
libbcpg-java-doc_1.49+dfsg-3+deb8u2
libbcprov-java_1.49+dfsg-3+deb8u2

145299 - SuSE SLES 11 SP4 SUSE-SU-2017:1030-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7741, CVE-2017-7742

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1030-1

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-April/002804.html

SuSE SLES 11 SP4
i586
libsndfile-1.0.20-2.13.1

x86_64
libsndfile-32bit-1.0.20-2.13.1
libsndfile-1.0.20-2.13.1

145301 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1003-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5844

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1003-1

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-April/002798.html

SuSE SLED 12 SP2
x86_64
gstreamer-0_10-plugins-base-debuginfo-0.10.36-17.13
gstreamer-0_10-plugins-base-0.10.36-17.13
libgstinterfaces-0_10-0-debuginfo-0.10.36-17.13
libgstinterfaces-0_10-0-0.10.36-17.13
libgstapp-0_10-0-debuginfo-32bit-0.10.36-17.13
libgstinterfaces-0_10-0-32bit-0.10.36-17.13
gstreamer-0_10-plugins-base-debugsource-0.10.36-17.13
libgstapp-0_10-0-0.10.36-17.13
gstreamer-0_10-plugins-base-debuginfo-32bit-0.10.36-17.13
libgstinterfaces-0_10-0-debuginfo-32bit-0.10.36-17.13
libgstapp-0_10-0-debuginfo-0.10.36-17.13
libgstapp-0_10-0-32bit-0.10.36-17.13
gstreamer-0_10-plugins-base-32bit-0.10.36-17.13

noarch
gstreamer-0_10-plugins-base-lang-0.10.36-17.13

SuSE SLES 12 SP2
x86_64
libgstinterfaces-0_10-0-32bit-0.10.36-17.13
gstreamer-0_10-plugins-base-32bit-0.10.36-17.13
libgstapp-0_10-0-32bit-0.10.36-17.13
libgstinterfaces-0_10-0-debuginfo-32bit-0.10.36-17.13
gstreamer-0_10-plugins-base-debuginfo-32bit-0.10.36-17.13
gstreamer-0_10-plugins-base-debugsource-0.10.36-17.13
libgstapp-0_10-0-debuginfo-32bit-0.10.36-17.13

145302 - SuSE SLES 11 SP4 SUSE-SU-2017:1000-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2775, CVE-2016-6170, CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1000-1

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-April/002797.html

SuSE SLES 11 SP4
i586
bind-chrootenv-9.9.6P1-0.44.1
bind-doc-9.9.6P1-0.44.1
bind-libs-9.9.6P1-0.44.1
bind-utils-9.9.6P1-0.44.1
bind-9.9.6P1-0.44.1

x86_64
bind-9.9.6P1-0.44.1
bind-doc-9.9.6P1-0.44.1
bind-chrootenv-9.9.6P1-0.44.1
bind-libs-32bit-9.9.6P1-0.44.1
bind-libs-9.9.6P1-0.44.1
bind-utils-9.9.6P1-0.44.1

145308 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:1040-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7586, CVE-2017-7741, CVE-2017-7742

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1040-1

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-April/002806.html

SuSE SLED 12 SP1
x86_64
libsndfile1-debuginfo-32bit-1.0.25-28.1
libsndfile1-32bit-1.0.25-28.1
libsndfile1-debuginfo-1.0.25-28.1
libsndfile1-1.0.25-28.1
libsndfile-debugsource-1.0.25-28.1

SuSE SLES 12 SP2
x86_64
libsndfile1-debuginfo-32bit-1.0.25-28.1
libsndfile1-32bit-1.0.25-28.1
libsndfile1-debuginfo-1.0.25-28.1
libsndfile1-1.0.25-28.1
libsndfile-debugsource-1.0.25-28.1

SuSE SLED 12 SP2
x86_64
libsndfile1-debuginfo-32bit-1.0.25-28.1
libsndfile1-32bit-1.0.25-28.1
libsndfile1-debuginfo-1.0.25-28.1
libsndfile1-1.0.25-28.1
libsndfile-debugsource-1.0.25-28.1

SuSE SLES 12 SP1
x86_64
libsndfile1-debuginfo-32bit-1.0.25-28.1
libsndfile1-32bit-1.0.25-28.1
libsndfile1-debuginfo-1.0.25-28.1
libsndfile1-1.0.25-28.1
libsndfile-debugsource-1.0.25-28.1

145313 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:1012-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5844

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1012-1

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-April/002802.html

SuSE SLES 12 SP1
x86_64
libgstapp-0_10-0-debuginfo-32bit-0.10.36-11.6.9
gstreamer-0_10-plugins-base-debuginfo-32bit-0.10.36-11.6.9
libgstinterfaces-0_10-0-debuginfo-32bit-0.10.36-11.6.9
libgstapp-0_10-0-32bit-0.10.36-11.6.9
libgstinterfaces-0_10-0-32bit-0.10.36-11.6.9
gstreamer-0_10-plugins-base-32bit-0.10.36-11.6.9

SuSE SLED 12 SP1
x86_64
gstreamer-0_10-plugins-base-32bit-0.10.36-11.6.9
libgstapp-0_10-0-debuginfo-32bit-0.10.36-11.6.9
gstreamer-0_10-plugins-base-debuginfo-0.10.36-11.6.9
libgstinterfaces-0_10-0-32bit-0.10.36-11.6.9
libgstapp-0_10-0-32bit-0.10.36-11.6.9
gstreamer-0_10-plugins-base-0.10.36-11.6.9
libgstinterfaces-0_10-0-0.10.36-11.6.9
libgstapp-0_10-0-0.10.36-11.6.9
libgstinterfaces-0_10-0-debuginfo-32bit-0.10.36-11.6.9
gstreamer-0_10-plugins-base-debuginfo-32bit-0.10.36-11.6.9
libgstapp-0_10-0-debuginfo-0.10.36-11.6.9
gstreamer-0_10-plugins-base-debugsource-0.10.36-11.6.9
libgstinterfaces-0_10-0-debuginfo-0.10.36-11.6.9

noarch
gstreamer-0_10-plugins-base-lang-0.10.36-11.6.9

145314 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0998-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2775, CVE-2016-6170, CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0998-1

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-April/002795.html

SuSE SLED 12 SP1
x86_64
bind-utils-debuginfo-9.9.9P1-59.1
bind-debuginfo-9.9.9P1-59.1
bind-libs-9.9.9P1-59.1
bind-libs-debuginfo-9.9.9P1-59.1
bind-libs-32bit-9.9.9P1-59.1
bind-debugsource-9.9.9P1-59.1
bind-utils-9.9.9P1-59.1
bind-libs-debuginfo-32bit-9.9.9P1-59.1

SuSE SLES 12 SP2
noarch
bind-doc-9.9.9P1-59.1

x86_64
bind-utils-debuginfo-9.9.9P1-59.1
bind-libs-9.9.9P1-59.1
bind-9.9.9P1-59.1
bind-libs-debuginfo-9.9.9P1-59.1
bind-libs-32bit-9.9.9P1-59.1
bind-debugsource-9.9.9P1-59.1

bind-utils-9.9.9P1-59.1
bind-libs-debuginfo-32bit-9.9.9P1-59.1
bind-chrootenv-9.9.9P1-59.1
bind-debuginfo-9.9.9P1-59.1

SuSE SLED 12 SP2
x86_64
bind-utils-debuginfo-9.9.9P1-59.1
bind-debuginfo-9.9.9P1-59.1
bind-libs-9.9.9P1-59.1
bind-libs-debuginfo-9.9.9P1-59.1
bind-libs-32bit-9.9.9P1-59.1
bind-debugsource-9.9.9P1-59.1
bind-utils-9.9.9P1-59.1
bind-libs-debuginfo-32bit-9.9.9P1-59.1

SuSE SLES 12 SP1
noarch
bind-doc-9.9.9P1-59.1

x86_64
bind-utils-debuginfo-9.9.9P1-59.1
bind-libs-9.9.9P1-59.1
bind-9.9.9P1-59.1
bind-libs-debuginfo-9.9.9P1-59.1
bind-libs-32bit-9.9.9P1-59.1
bind-debugsource-9.9.9P1-59.1
bind-utils-9.9.9P1-59.1
bind-libs-debuginfo-32bit-9.9.9P1-59.1
bind-chrootenv-9.9.9P1-59.1
bind-debuginfo-9.9.9P1-59.1

191941 - Fedora Linux 25 FEDORA-2017-72a971ccf0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7586

Description

The scan detected that the host is missing the following update:
FEDORA-2017-72a971ccf0

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/2017/4/?count=200&page=2

Fedora Core 25

libsndfile-1.0.28-1.fc25

191948 - Fedora Linux 26 FEDORA-2017-a2a4f8d8a1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7586

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a2a4f8d8a1

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/2017/4/?count=200&page=2

Fedora Core 26

libsndfile-1.0.28-1.fc26

191953 - Fedora Linux 25 FEDORA-2017-2d11503623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10221

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2d11503623

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/2017/4/?count=200&page=1

Fedora Core 25

mupdf-1.10a-5.fc25

191957 - Fedora Linux 24 FEDORA-2017-97e65f13bb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5591

Description

The scan detected that the host is missing the following update:
FEDORA-2017-97e65f13bb

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/2017/4/?count=200&page=3

Fedora Core 24

python-sleekxmpp-1.3.2-1.fc24

191964 - Fedora Linux 24 FEDORA-2017-f676ecb20d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7586

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f676ecb20d

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/2017/4/?count=200&page=1

Fedora Core 24

libsndfile-1.0.28-1.fc24

191965 - Fedora Linux 25 FEDORA-2017-99ad80f109 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5591

Description

The scan detected that the host is missing the following update:
FEDORA-2017-99ad80f109

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/2017/4/?count=200&page=3

Fedora Core 25

python-sleekxmpp-1.3.2-1.fc25

191973 - Fedora Linux 26 FEDORA-2017-68bd2a916e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5591

Description

The scan detected that the host is missing the following update:
FEDORA-2017-68bd2a916e

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/2017/4/?count=200&page=3

Fedora Core 26

python-sleekxmpp-1.3.2-1.fc26

33367 - Oracle Solaris 144229-02 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:
144229-02

Observation

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

https://getupdates.oracle.com/readme/144229-02

X11 6.6.2: libpixman patch

SOLARIS_10

SUNWpixman:6.6.2.4099,REV=0.2009.06.21

33368 - Oracle Solaris 144230-02 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:
144230-02

Observation

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

https://getupdates.oracle.com/readme/144230-02

X11 6.6.2(x86): libpixman patch

SOLARIS_10_x86

SUNWpixman:6.6.2.4099,REV=0.2009.06.21

37554 - IBM AIX IV90234 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV90234

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV90234

7200-01
bos.mp64 < 7.2.1.1

37555 - IBM AIX IV91006 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91006

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91006

6100-09
bos.net.tcp.client < 6.1.9.201

37556 - IBM AIX IV91007 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91007

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91007

7100-03
bos.net.tcp.client < 7.1.3.49

37557 - IBM AIX IV91008 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91008

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91008

7100-04
bos.net.tcp.client < 7.1.4.31

37558 - IBM AIX IV91214 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91214

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91214

7100-03
bos.net.tcp.client < 7.1.3.49

37559 - IBM AIX IV91254 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91254

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91254

6100-09
bos.net.tcp.client < 6.1.9.201

37560 - IBM AIX IV91255 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91255

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91255

7100-04
bos.net.tcp.client < 7.1.4.31

37561 - IBM AIX IV91256 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91256

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91256

7200-00
bos.net.tcp.bind_utils < 7.2.0.3

37562 - IBM AIX IV91257 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91257

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91257

7200-01
bos.net.tcp.bind_utils < 7.2.1.2

37568 - IBM AIX IV91456 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91456

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91456

7200-00
bos.mp64 < 7.2.0.4

37569 - IBM AIX IV91487 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91487

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91487

7100-04
bos.mp64 < 7.1.4.32

37570 - IBM AIX IV91488 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91488

Observation

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

For more information see:

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91488

7100-03
bos.mp64 < 7.1.3.50

37571 - IBM AIX IV91803 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91803

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91803

6100-09
bos.net.tcp.client < 6.1.9.201

37572 - IBM AIX IV91951 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV91951

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV91951

7100-04
bos.net.tcp.client < 7.1.4.31

37573 - IBM AIX IV92067 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92067

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92067

7200-01
bos.net.tcp.ntpd < 7.2.1.1

37574 - IBM AIX IV92192 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92192

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92192

7200-00
bos.net.tcp.ntpd < 7.2.0.3

37575 - IBM AIX IV92193 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92193

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92193

7100-03
bos.net.tcp.client < 7.1.3.49

37576 - IBM AIX IV92238 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92238

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92238

6100-09
bos.net.tcp.client < 6.1.9.201

37577 - IBM AIX IV92240 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92240

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92240

7100-04
bos.net.tcp.client < 7.1.4.31

37578 - IBM AIX IV92241 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92241

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92241

7200-00
bos.net.tcp.client_core < 7.2.0.3

37579 - IBM AIX IV92242 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92242

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92242

7200-01
bos.net.tcp.client_core < 7.2.1.1

37580 - IBM AIX IV92250 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV92250

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV92250

7100-03
bos.net.tcp.client < 7.1.3.49

88858 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-103-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
SSA:2017-103-01

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.556633

Slackware 14.0
x86_64
bind-9.9.9_P8-x86_64-1

Slackware 13.37
x86_64
bind-9.9.9_P8-x86_64-1

Slackware 14.1
x86_64
bind-9.9.9_P8-x86_64-1

Slackware 13.1
x86_64
bind-9.9.9_P8-x86_64-1

Slackware 14.2
x86_64
bind-9.10.4_P8-x86_64-1

i586
bind-9.10.4_P8-i586-1

Slackware 13.0
x86_64
bind-9.9.9_P8-x86_64-1

182326 - FreeBSD BIND Multiple Vulnerabilities (c6861494-1ffb-11e7-934d-d05099c0ae8c)

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
BIND -- multiple vulnerabilities (c6861494-1ffb-11e7-934d-d05099c0ae8c)

Observation

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

http://www.vuxml.org/freebsd/c6861494-1ffb-11e7-934d-d05099c0ae8c.html

Affected packages:
bind99 < 9.9.9P8
bind910 < 9.10.4P8
bind911 < 9.11.0P5
bind9-devel <= 9.12.0.a.2017.03.25

191947 - Fedora Linux 26 FEDORA-2017-05cb6287b7 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-2017-05cb6287b7

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/2017/4/?count=200&page=3

Fedora Core 26

mediawiki-1.28.1-2.fc26

191950 - Fedora Linux 26 FEDORA-2017-49f828d4b1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

The scan detected that the host is missing the following update:
FEDORA-2017-49f828d4b1

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/2017/4/?count=200&page=3

Fedora Core 26

chromium-57.0.2987.133-1.fc26

191954 - Fedora Linux 24 FEDORA-2017-97fb93e1d1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
FEDORA-2017-97fb93e1d1

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/2017/4/?count=200&page=2

Fedora Core 24

samba-4.4.13-1.fc24

191955 - Fedora Linux 26 FEDORA-2017-d5ef38bf2c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9587, CVE-2017-7466

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d5ef38bf2c

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/2017/4/?count=200&page=1

Fedora Core 26

ansible-2.3.0.0-1.fc26

191961 - Fedora Linux 25 FEDORA-2017-3fb95ed01f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-0361, CVE-2017-0362, CVE-2017-0363, CVE-2017-0364, CVE-2017-0365, CVE-2017-0366, CVE-2017-0367, CVE-2017-0368, CVE-2017-0369, CVE-2017-0370, CVE-2017-0372

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3fb95ed01f

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/2017/4/?count=200&page=2

Fedora Core 25

mediawiki-1.27.2-1.fc25

145305 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:1042-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9586, CVE-2017-7407

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1042-1

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-April/002808.html

SuSE SLED 12 SP1
x86_64
libcurl4-debuginfo-32bit-7.37.0-36.1

curl-debugsource-7.37.0-36.1
libcurl4-debuginfo-7.37.0-36.1
libcurl4-32bit-7.37.0-36.1
libcurl4-7.37.0-36.1
curl-debuginfo-7.37.0-36.1
curl-7.37.0-36.1

SuSE SLES 12 SP2
x86_64
libcurl4-debuginfo-32bit-7.37.0-36.1
curl-debugsource-7.37.0-36.1
libcurl4-debuginfo-7.37.0-36.1
libcurl4-32bit-7.37.0-36.1
libcurl4-7.37.0-36.1
curl-debuginfo-7.37.0-36.1
curl-7.37.0-36.1

SuSE SLED 12 SP2
x86_64
libcurl4-debuginfo-32bit-7.37.0-36.1
curl-debugsource-7.37.0-36.1
libcurl4-debuginfo-7.37.0-36.1
libcurl4-32bit-7.37.0-36.1
libcurl4-7.37.0-36.1
curl-debuginfo-7.37.0-36.1
curl-7.37.0-36.1

SuSE SLES 12 SP1
x86_64
libcurl4-debuginfo-32bit-7.37.0-36.1
curl-debugsource-7.37.0-36.1
libcurl4-debuginfo-7.37.0-36.1
libcurl4-32bit-7.37.0-36.1
libcurl4-7.37.0-36.1
curl-debuginfo-7.37.0-36.1
curl-7.37.0-36.1

145306 - SuSE SLES 11 SP4 SUSE-SU-2017:1043-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9586, CVE-2017-7407

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1043-1

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-April/002809.html

SuSE SLES 11 SP4
i586
curl-7.19.7-1.69.1
libcurl4-7.19.7-1.69.1

x86_64
curl-7.19.7-1.69.1
libcurl4-32bit-7.19.7-1.69.1
libcurl4-7.19.7-1.69.1

191958 - Fedora Linux 24 FEDORA-2017-e15e37b689 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7418

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e15e37b689

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/2017/4/?count=200&page=1

Fedora Core 24

proftpd-1.3.5e-1.fc24

191970 - Fedora Linux 26 FEDORA-2017-5a01498b4b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7418

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5a01498b4b

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/2017/4/?count=200&page=2

Fedora Core 26

proftpd-1.3.5e-1.fc26

135176 - Oracle Solaris 11.3.17.5.0 Update Is Not Installed (CVE-2017-3474)

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

Risk Level: Low

CVE: CVE-2017-3474

Description

The scan detected that the host is missing the following update:
SRU 11.3.17.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135177 - Oracle Solaris 11.3.17.5.0 Update Is Not Installed (CVE-2017-3497)

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

Risk Level: Low

CVE: CVE-2017-3497

Description

The scan detected that the host is missing the following update:
SRU 11.3.17.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135178 - Oracle Solaris 11.3.19.5.0 Update Is Not Installed (CVE-2017-3498)

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

Risk Level: Low

CVE: CVE-2017-3498

Description

The scan detected that the host is missing the following update:
SRU 11.3.19.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135179 - Oracle Solaris 11.3.18.6.0 Update Is Not Installed (CVE-2017-3510)

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

Risk Level: Low

CVE: CVE-2017-3510

Description

The scan detected that the host is missing the following update:
SRU 11.3.18.6.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135180 - Oracle Solaris 11.3.18.6.0 Update Is Not Installed (CVE-2017-3516)

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

Risk Level: Low

CVE: CVE-2017-3516

Description

The scan detected that the host is missing the following update:
SRU 11.3.18.6.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135181 - Oracle Solaris 11.3.17.5.0 Update Is Not Installed (CVE-2017-3551)

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

Risk Level: Low

CVE: CVE-2017-3551

Description

The scan detected that the host is missing the following update:
SRU 11.3.17.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135182 - Oracle Solaris 11.3.19.5.0 Update Is Not Installed (CVE-2017-3564)

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

Risk Level: Low

CVE: CVE-2017-3564

Description

The scan detected that the host is missing the following update:
SRU 11.3.19.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

135183 - Oracle Solaris 11.3.19.5.0 Update Is Not Installed (CVE-2017-3565)

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

Risk Level: Low

CVE: CVE-2017-3565

Description

The scan detected that the host is missing the following update:
SRU 11.3.19.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2252071.1&_adf.ctrl-state=t14x56woa_4&_afrLoop=324611163272474

21704 - Double Pulsar Backdoor SMB Detection

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

A DOUBLEPULSAR backdoor is present in the remote Windows host.

Observation

DOUBLEPULSAR is a backdoor developed by NSA.

A DOUBLEPULSAR backdoor is present in the remote Windows host. Once a Windows system is infected by DOUBLEPULSAR backdoor, a remote attacker can use SMB as a covert channel to exfiltrate data, or execute arbitrary code.

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.

191118 - Fedora Linux 24 FEDORA-2016-145afea99e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6299

Update Details

Risk is updated

191135 - Fedora Linux 25 FEDORA-2016-34e61fa48d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6299

Update Details

Risk is updated

191155 - Fedora Linux 23 FEDORA-2016-5a12527790 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-6299

Update Details
Risk is updated

130458 - Debian Linux 7.0, 8.0 DSA-3540-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2347

Update Details
Risk is updated

132313 - Oracle VM OVMSA-2016-0170 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7032, CVE-2016-7076

Update Details
Risk 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
Risk is updated

144531 - SuSE Linux 13.2 openSUSE-SU-2016:1027-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2347

Update Details
Risk is updated

144537 - SuSE SLED 12, 12 SP1 SUSE-SU-2016:1091-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2347

Update Details
Risk is updated

144950 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2654-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8602

Update Details
Risk is updated

144978 - SuSE SLES 11 SP4 SUSE-SU-2016:2723-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8602

Update Details
Risk is updated

145010 - SuSE Linux 13.2 openSUSE-SU-2016:2878-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7032, CVE-2016-7076

Update Details
Risk is updated

145020 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:2893-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7032, CVE-2016-7076

Update Details
Risk is updated

145022 - SuSE SLES 11 SP4 SUSE-SU-2016:2891-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7032, CVE-2016-7076

Update Details
Risk is updated

145029 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2904-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-9680, CVE-2016-7032, CVE-2016-7076

Update Details

Risk is updated

160177 - CentOS 6 CESA-2016-2872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

Update Details

Risk is updated

163236 - Oracle Enterprise Linux ELSA-2016-2872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

Update Details

Risk is updated

170758 - Amazon Linux AMI ALAS-2017-780 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

Update Details

Risk is updated

175071 - Scientific Linux Security ERRATA Moderate: sudo on SL6.x, SL7.x i386/x86_64 (1612-16295)

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

Update Details

Risk is updated

178412 - Gentoo Linux GLSA-201702-31 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7976, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

Update Details

Risk is updated

191327 - Fedora Linux 24 FEDORA-2016-3dad5dfd03 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7977, CVE-2016-8602

Update Details
Risk is updated

191382 - Fedora Linux 25 FEDORA-2016-62f2b66ed1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7977, CVE-2016-8602

Update Details
Risk is updated

191412 - Fedora Linux 23 FEDORA-2016-15d4c05a19 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-7977, CVE-2016-8602

Update Details
Risk is updated

191865 - Fedora Linux 24 FEDORA-2017-922652dd9c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2784

Update Details
Risk is updated

191877 - Fedora Linux 25 FEDORA-2017-9ed1b89530 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2784

Update Details
Risk is updated

191889 - Fedora Linux 26 FEDORA-2017-718154e0f2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2784

Update Details
Risk is updated

21588 - (MSPT-Apr2017) Microsoft Outlook Parsing Remote Code Execution (CVE-2017-0199)

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

Risk Level: Medium

CVE: CVE-2017-0199

Update Details

Risk is updated

185572 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3193-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6489

Update Details

Risk is updated

191076 - Fedora Linux 23 FEDORA-2016-ce1678471e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6331, CVE-2016-6332, CVE-2016-6333, CVE-2016-6334, CVE-2016-6335, CVE-2016-6336

Update Details

Risk is updated

191080 - Fedora Linux 24 FEDORA-2016-af3b0af887 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6331, CVE-2016-6332, CVE-2016-6333, CVE-2016-6334, CVE-2016-6335, CVE-2016-6336

Update Details

Risk is updated

191086 - Fedora Linux 25 FEDORA-2016-9299ce1c7d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6331, CVE-2016-6332, CVE-2016-6333, CVE-2016-6334, CVE-2016-6335, CVE-2016-6336

Update Details

Risk is updated

191365 - Fedora Linux 25 FEDORA-2016-762cb57c92 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6489

Update Details

Risk is updated

20601 - (SYM16-015) Symantec Endpoint Protection Decomposer Engine Multiple Vulnerabilities

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-5309, CVE-2016-5310

Update Details

Risk is updated

20602 - (SYM16-015) Symantec Mail Security for Microsoft Exchange Decomposer Engine Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-5309, CVE-2016-5310

Update Details

Risk is updated

20604 - (SYM16-015) Symantec Messaging Gateway Decomposer Engine Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-5309, CVE-2016-5310

Update Details

Risk is updated

20605 - (SYM16-015) Symantec Messaging Gateway Decomposer Engine Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5309, CVE-2016-5310

Update Details

Risk is updated

20613 - (SYM16-015) Symantec Mail Security for Domino Decomposer Engine Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-5309, CVE-2016-5310

Update Details

Risk 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: Low
CVE: CVE-2016-4455

Update Details
Risk is updated

141352 - Red Hat Enterprise Linux RHSA-2016-2597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-5410

Update Details
Risk is updated

141506 - Red Hat Enterprise Linux RHSA-2017-0698 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-4455

Update Details
Risk is updated

163216 - Oracle Enterprise Linux ELSA-2016-2597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-5410

Update Details
Risk is updated

175054 - Scientific Linux Security ERRATA Moderate: firewalld on SL7.x (noarch) (1612-10449)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Low
CVE: CVE-2016-5410

Update Details
Risk is updated

175092 - Scientific Linux Security ERRATA Moderate: subscription-manager on SL7.x x86_64 (1701-2848)

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

CVE: CVE-2016-4455

Update Details

Risk is updated

175148 - Scientific Linux Security ERRATA Moderate: subscription-manager on SL6.x i386/x86_64 (1704-4522)

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

Risk Level: Low

CVE: CVE-2016-4455

Update Details

Risk is updated

178379 - Gentoo Linux GLSA-201701-70 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5410

Update Details

Risk is updated

191010 - Fedora Linux 24 FEDORA-2016-de55d2c2c9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5410

Update Details

Risk is updated

191072 - Fedora Linux 25 FEDORA-2016-4dedc6ec3d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5410

Update Details

Risk is updated

45000 - ShellLogon.fasl3

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

45001 - ShellInitialize.fasl3

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70046 - macosx.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70048 - adobe.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70084 - tomcat.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com/

Multi-National Phone Support available here:

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

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