

MCAFFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

194793 - Fedora Linux 28 FEDORA-2019-e0eb3d797e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15686, CVE-2018-15687, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e0eb3d797e

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/2019/2/?count=200&page=1>

Fedora Core 28

systemd-238-11.gita76ee90.fc28

194794 - Fedora Linux 28 FEDORA-2019-3da64f3e61 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16880, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3da64f3e61

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/2019/2/?count=200&page=1>

Fedora Core 28

kernel-tools-4.20.8-100.fc28

kernel-headers-4.20.8-100.fc28
kernel-4.20.8-100.fc28

147624 - SuSE Linux 15.0 openSUSE-SU-2019:0208-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16873, CVE-2018-16874, CVE-2018-16875, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0208-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00103.html>

SuSE Linux 15.0
x86_64
runc-1.0.0~rc6-lp150.2.3.1
runc-debuginfo-1.0.0~rc6-lp150.2.3.1

noarch
runc-test-1.0.0~rc6-lp150.2.3.1

147635 - SuSE Linux 42.3 openSUSE-SU-2019:0201-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0201-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00096.html>

SuSE Linux 42.3
i586
docker-runc-kubic-debuginfo-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-debugsource-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-debuginfo-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-kubic-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-kubic-debugsource-1.0.0rc5+gitr3562_69663f0bd4b6-8.1

noarch
docker-runc-test-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-kubic-test-1.0.0rc5+gitr3562_69663f0bd4b6-8.1

x86_64
docker-runc-kubic-debuginfo-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-debugsource-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-debuginfo-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-kubic-1.0.0rc5+gitr3562_69663f0bd4b6-8.1
docker-runc-kubic-debugsource-1.0.0rc5+gitr3562_69663f0bd4b6-8.1

194779 - Fedora Linux 29 FEDORA-2019-df2e68aa6b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20699, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-df2e68aa6b

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/2019/2/?count=200&page=1>

Fedora Core 29

docker-1.13.1-65.git1185cfd.fc29

194789 - Fedora Linux 29 FEDORA-2019-352d4b9cd8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-352d4b9cd8

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/2019/2/?count=200&page=1>

Fedora Core 29

moby-engine-18.06.0-2.ce.git0ffa825.fc29

194791 - Fedora Linux 28 FEDORA-2019-829524f28f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-829524f28f

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/2019/2/?count=200&page=1>

Fedora Core 28

moby-engine-18.06.0-2.ce.git0ffa825.fc28

194795 - Fedora Linux 29 FEDORA-2019-3f19f13ecd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20699, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3f19f13ecd

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/2019/2/?count=200&page=1>

Fedora Core 29

runc-1.0.0-68.dev.git6635b4f.fc29

24774 - (JSA10901) Juniper Junos OS EX2300 and EX3400 Series Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0002

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in stateless firewall filter configuration. Successful exploitation could allow an attacker to bypass security restrictions on the target system.

24749 - (JSA10910) Juniper Junos OS SRX Series Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0010

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in the Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in Junos SRX Series Service Gateway configured for Unified Threat Management component. Successful exploitation could allow an attacker to cause a denial of service condition on the targeted system.

24755 - (JSA10903) Juniper Junos OS vMX Series Predictable IP ID Sequence Numbers Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0007

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw is due to a predictable IP ID Sequence Number. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

24772 - (HPESBUX03908) HP-UX Web Server Suite running Apache Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-4975, CVE-2017-3167, CVE-2017-3169, CVE-2017-7659, CVE-2017-7668, CVE-2017-7679, CVE-2017-9788, CVE-2017-9789

Description

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

Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in the Web Server component. Successful exploitation could allow an attacker to obtain sensitive information, bypass authentication, cause a denial of service and other impacts.

24773 - (HPESBUX03909) HP-UX Web Server Suite running Apache Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-15710, CVE-2017-15715, CVE-2017-9798, CVE-2018-11763, CVE-2018-1283, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-2018-1312, CVE-2018-1333

Description

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

Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in the Web Server component. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service and other impacts.

24776 - (JSA10904) Juniper Junos OS libbsdxml XML Parser Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-1283

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in the Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in Junos expat XML processing library component. Successful exploitation could allow an attacker to cause a denial of service condition on the targeted system.

24777 - (SB10269) McAfee Threat Intelligence Exchange Server Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0732, CVE-2018-15473, CVE-2018-15919, CVE-2018-5391, CVE-2018-5407

Description

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange Server.

Observation

McAfee Threat Intelligence Exchange Server is a real-time threat detection and response software.

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange Server. The flaws lie in Kernel and SSH components. Successful exploitation could allow a remote attacker to cause a denial of service, and obtain sensitive information.

24779 - (HPESBHF03907) HPE Integrated Lights-Out Remote Cross-Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-2018-7117

Description

A vulnerability is present in some versions of HPE Integrated Lights-Out.

Observation

HPE Integrated Lights-Out is a Hewlett-Packard proprietary embedded server management technology.

A vulnerability is present in some versions of HPE Integrated Lights-Out. The flaw is in web user interface component. Successful exploitation could allow a local attacker to disclose sensitive information and or cause denial of service condition.

24783 - (HT209520) Apple iOS Multiple Vulnerabilities Prior To 12.1.4

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2019-6223, CVE-2019-7286, CVE-2019-7287, CVE-2019-7288

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

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

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in many components. Successful exploitation could allow an attacker to cause remote code execution, privilege escalation on the target.

24787 - (APSB19-13) Information Disclosure In Adobe Acrobat and Reader

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

Risk Level: High

CVE: CVE-2019-7815

Description

A vulnerability is present in some versions of Adobe Reader and Acrobat.

Observation

Adobe Reader and Acrobat are popular applications used to handle PDF files.

A vulnerability is present in some versions of Adobe Reader and Acrobat. The flaw lies in the undetermined component. Successful exploitation could allow an attacker to obtain sensitive information.

The update provided by Adobe bulletin APSB19-13 resolves the issue.

131296 - Debian Linux 9.0 DSA-4396-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10855, CVE-2018-10875, CVE-2018-16837, CVE-2018-16876, CVE-2019-3828

Description

The scan detected that the host is missing the following update:
DSA-4396-1

Observation

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

<http://www.debian.org/security/2019/dsa-4396>

Debian 9.0

all

ansible_2.2.1.0-2+deb9u1

131297 - Debian Linux 9.0 DSA-4394-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20174, CVE-2018-20175, CVE-2018-20176, CVE-2018-20177, CVE-2018-20178, CVE-2018-20179, CVE-2018-20180, CVE-2018-20181, CVE-2018-20182, CVE-2018-8791, CVE-2018-8792, CVE-2018-8793, CVE-2018-8794, CVE-2018-8795, CVE-2018-8796, CVE-2018-8797, CVE-2018-8798, CVE-2018-8799, CVE-2018-8800

Description

The scan detected that the host is missing the following update:
DSA-4394-1

Observation

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

<http://www.debian.org/security/2019/dsa-4394>

Debian 9.0
all
rdesktop_1.8.4-1~deb9u1

131298 - Debian Linux 9.0 DSA-4392-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18356, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505, CVE-2018-18509, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
DSA-4392-1

Observation

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

<http://www.debian.org/security/2019/dsa-4392>

Debian 9.0
all
thunderbird_1:60.5.1-1~deb9u1

147627 - SuSE Linux 15.0 openSUSE-SU-2019:0196-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20748, CVE-2018-20749, CVE-2018-20750

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0196-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00085.html>

SuSE Linux 15.0

x86_64

LibVNCServer-devel-0.9.10-lp150.3.6.1

libvncclient0-0.9.10-lp150.3.6.1

LibVNCServer-debugsource-0.9.10-lp150.3.6.1

libvncserver0-0.9.10-lp150.3.6.1

libvncclient0-debuginfo-0.9.10-lp150.3.6.1

libvncserver0-debuginfo-0.9.10-lp150.3.6.1

i586

LibVNCServer-devel-0.9.10-lp150.3.6.1

libvncclient0-0.9.10-lp150.3.6.1

LibVNCServer-debugsource-0.9.10-lp150.3.6.1

libvncserver0-0.9.10-lp150.3.6.1

libvncclient0-debuginfo-0.9.10-lp150.3.6.1

libvncserver0-debuginfo-0.9.10-lp150.3.6.1

147629 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0339-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

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

SUSE-SU-2019:0339-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005111.html>

SuSE SLED 12 SP4

x86_64

libcurl4-32bit-7.60.0-4.3.1

libcurl4-debuginfo-32bit-7.60.0-4.3.1

curl-debuginfo-7.60.0-4.3.1

curl-7.60.0-4.3.1

libcurl4-debuginfo-7.60.0-4.3.1

libcurl4-7.60.0-4.3.1

curl-debugsource-7.60.0-4.3.1

SuSE SLES 12 SP4

x86_64

libcurl4-7.60.0-4.3.1

libcurl4-debuginfo-32bit-7.60.0-4.3.1

curl-debuginfo-7.60.0-4.3.1

curl-7.60.0-4.3.1

libcurl4-debuginfo-7.60.0-4.3.1

curl-debugsource-7.60.0-4.3.1

libcurl4-32bit-7.60.0-4.3.1

147630 - SuSE Linux 42.3 openSUSE-SU-2019:0182-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5824, CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0182-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00073.html>

SuSE Linux 42.3

x86_64

MozillaThunderbird-translations-other-60.5.0-83.1

MozillaThunderbird-debugsource-60.5.0-83.1

MozillaThunderbird-60.5.0-83.1

MozillaThunderbird-buildsymbols-60.5.0-83.1

MozillaThunderbird-translations-common-60.5.0-83.1

MozillaThunderbird-debuginfo-60.5.0-83.1

147631 - SuSE Linux 15.0 openSUSE-SU-2019:0174-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0174-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00063.html>

SuSE Linux 15.0

x86_64

libcurl-devel-7.60.0-lp150.2.18.1

curl-mini-7.60.0-lp150.2.18.1

curl-7.60.0-lp150.2.18.1

curl-mini-debuginfo-7.60.0-lp150.2.18.1

curl-mini-debugsource-7.60.0-lp150.2.18.1

libcurl4-32bit-debuginfo-7.60.0-lp150.2.18.1

libcurl4-7.60.0-lp150.2.18.1

libcurl4-mini-7.60.0-lp150.2.18.1

curl-debuginfo-7.60.0-lp150.2.18.1

libcurl4-32bit-7.60.0-lp150.2.18.1

curl-debugsource-7.60.0-lp150.2.18.1

libcurl4-debuginfo-7.60.0-lp150.2.18.1

libcurl-mini-devel-7.60.0-lp150.2.18.1

libcurl4-mini-debuginfo-7.60.0-lp150.2.18.1

libcurl-devel-32bit-7.60.0-lp150.2.18.1

i586
libcurl-mini-devel-7.60.0-lp150.2.18.1
curl-mini-7.60.0-lp150.2.18.1
libcurl4-mini-7.60.0-lp150.2.18.1
libcurl-devel-7.60.0-lp150.2.18.1
curl-mini-debugsource-7.60.0-lp150.2.18.1
curl-mini-debuginfo-7.60.0-lp150.2.18.1
curl-debugsource-7.60.0-lp150.2.18.1
libcurl4-7.60.0-lp150.2.18.1
curl-7.60.0-lp150.2.18.1
libcurl4-debuginfo-7.60.0-lp150.2.18.1
libcurl4-mini-debuginfo-7.60.0-lp150.2.18.1
curl-debuginfo-7.60.0-lp150.2.18.1

147632 - SuSE Linux 15.0 openSUSE-SU-2019:0184-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5010

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0184-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00071.html>

SuSE Linux 15.0

i586
python-gdbm-debuginfo-2.7.14-lp150.6.6.1
python-base-debuginfo-2.7.14-lp150.6.6.1
libpython2_7-1_0-debuginfo-2.7.14-lp150.6.6.1
python-gdbm-2.7.14-lp150.6.6.1
python-tk-2.7.14-lp150.6.6.1
python-xml-debuginfo-2.7.14-lp150.6.6.1
python-2.7.14-lp150.6.6.1
python-debuginfo-2.7.14-lp150.6.6.1
python-base-debugsource-2.7.14-lp150.6.6.1
python-devel-2.7.14-lp150.6.6.1
python-base-2.7.14-lp150.6.6.1
python-curses-2.7.14-lp150.6.6.1
python-tk-debuginfo-2.7.14-lp150.6.6.1
libpython2_7-1_0-2.7.14-lp150.6.6.1
python-demo-2.7.14-lp150.6.6.1
python-curses-debuginfo-2.7.14-lp150.6.6.1
python-idle-2.7.14-lp150.6.6.1
python-debugsource-2.7.14-lp150.6.6.1
python-xml-2.7.14-lp150.6.6.1

noarch

python-doc-pdf-2.7.14-lp150.6.6.1
python-doc-2.7.14-lp150.6.6.1

x86_64

python-gdbm-debuginfo-2.7.14-lp150.6.6.1
python-base-debuginfo-2.7.14-lp150.6.6.1
libpython2_7-1_0-debuginfo-2.7.14-lp150.6.6.1
python-gdbm-2.7.14-lp150.6.6.1
python-tk-2.7.14-lp150.6.6.1
python-xml-debuginfo-2.7.14-lp150.6.6.1
python-2.7.14-lp150.6.6.1
python-debuginfo-2.7.14-lp150.6.6.1
python-base-debugsource-2.7.14-lp150.6.6.1
python-devel-2.7.14-lp150.6.6.1
python-32bit-2.7.14-lp150.6.6.1
python-base-2.7.14-lp150.6.6.1
python-curses-2.7.14-lp150.6.6.1
libpython2_7-1_0-32bit-debuginfo-2.7.14-lp150.6.6.1
python-tk-debuginfo-2.7.14-lp150.6.6.1
libpython2_7-1_0-2.7.14-lp150.6.6.1
python-demo-2.7.14-lp150.6.6.1
python-32bit-debuginfo-2.7.14-lp150.6.6.1
python-base-32bit-2.7.14-lp150.6.6.1
python-curses-debuginfo-2.7.14-lp150.6.6.1
libpython2_7-1_0-32bit-2.7.14-lp150.6.6.1
python-idle-2.7.14-lp150.6.6.1
python-base-32bit-debuginfo-2.7.14-lp150.6.6.1
python-debugsource-2.7.14-lp150.6.6.1
python-xml-2.7.14-lp150.6.6.1

147634 - SuSE Linux 15.0 openSUSE-SU-2019:0166-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20615

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0166-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00055.html>

SuSE Linux 15.0

x86_64

haproxy-1.8.17~git0.e89d25b2-lp150.2.9.1

haproxy-debugsource-1.8.17~git0.e89d25b2-lp150.2.9.1

haproxy-debuginfo-1.8.17~git0.e89d25b2-lp150.2.9.1

147637 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0419-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6446

Description

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

SUSE-SU-2019:0419-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005128.html>

SuSE SLED 12 SP3

x86_64
python-numpy-1.8.0-5.8.1
python-numpy-debuginfo-1.8.0-5.8.1
python-numpy-debugsource-1.8.0-5.8.1

SuSE SLED 12 SP4

x86_64
python-numpy-1.8.0-5.8.1
python-numpy-debuginfo-1.8.0-5.8.1
python-numpy-debugsource-1.8.0-5.8.1

SuSE SLES 12 SP4

x86_64
python-numpy-1.8.0-5.8.1
python-numpy-debuginfo-1.8.0-5.8.1
python-numpy-debugsource-1.8.0-5.8.1

SuSE SLES 12 SP3

x86_64
python-numpy-1.8.0-5.8.1
python-numpy-debuginfo-1.8.0-5.8.1
python-numpy-debugsource-1.8.0-5.8.1

147640 - SuSE Linux 42.3 openSUSE-SU-2019:0207-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19935, CVE-2019-6977, CVE-2019-6978

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0207-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00098.html>

SuSE Linux 42.3

i586
php7-dba-7.0.7-55.1
php7-xsl-7.0.7-55.1
php7-intl-debuginfo-7.0.7-55.1
php7-calendar-debuginfo-7.0.7-55.1
php7-sysvshm-7.0.7-55.1
php7-tidy-debuginfo-7.0.7-55.1
php7-sqlite-debuginfo-7.0.7-55.1

php7-imap-7.0.7-55.1
php7-iconv-7.0.7-55.1
php7-sockets-debuginfo-7.0.7-55.1
php7-pspell-7.0.7-55.1
php7-ctype-7.0.7-55.1
php7-dom-debuginfo-7.0.7-55.1
php7-pgsql-7.0.7-55.1
php7-mcrypt-debuginfo-7.0.7-55.1
php7-sysvsem-debuginfo-7.0.7-55.1
php7-zip-debuginfo-7.0.7-55.1
php7-sqlite-7.0.7-55.1
php7-bcmath-7.0.7-55.1
php7-devel-7.0.7-55.1
php7-zlib-debuginfo-7.0.7-55.1
php7-sockets-7.0.7-55.1
php7-bz2-debuginfo-7.0.7-55.1
php7-gmp-debuginfo-7.0.7-55.1
php7-openssl-7.0.7-55.1
php7-bz2-7.0.7-55.1
php7-mysql-7.0.7-55.1
php7-debuginfo-7.0.7-55.1
php7-curl-7.0.7-55.1
php7-exif-debuginfo-7.0.7-55.1
php7-fpm-debuginfo-7.0.7-55.1
php7-wddx-debuginfo-7.0.7-55.1
php7-phar-debuginfo-7.0.7-55.1
php7-odbc-7.0.7-55.1
php7-pgsql-debuginfo-7.0.7-55.1
php7-gettext-7.0.7-55.1
php7-shmop-debuginfo-7.0.7-55.1
php7-iconv-debuginfo-7.0.7-55.1
php7-gd-7.0.7-55.1
php7-pspell-debuginfo-7.0.7-55.1
php7-tokenizer-debuginfo-7.0.7-55.1
php7-mbstring-7.0.7-55.1
php7-exif-7.0.7-55.1
php7-calendar-7.0.7-55.1
php7-gd-debuginfo-7.0.7-55.1
php7-mbstring-debuginfo-7.0.7-55.1
php7-xmlwriter-debuginfo-7.0.7-55.1
php7-zlib-7.0.7-55.1
php7-dba-debuginfo-7.0.7-55.1
php7-debugsource-7.0.7-55.1
php7-pdo-debuginfo-7.0.7-55.1
php7-sysvshm-debuginfo-7.0.7-55.1
php7-sysvsem-7.0.7-55.1
php7-fpm-7.0.7-55.1
php7-ldap-7.0.7-55.1
php7-intl-7.0.7-55.1
php7-7.0.7-55.1
php7-json-7.0.7-55.1
php7-enchanted-debuginfo-7.0.7-55.1
php7-openssl-debuginfo-7.0.7-55.1
php7-zip-7.0.7-55.1
php7-shmop-7.0.7-55.1
php7-soap-7.0.7-55.1
php7-snmp-debuginfo-7.0.7-55.1
php7-pcntl-7.0.7-55.1
php7-soap-debuginfo-7.0.7-55.1
php7-readline-debuginfo-7.0.7-55.1

php7-fastcgi-7.0.7-55.1
php7-fileinfo-debuginfo-7.0.7-55.1
php7-opcache-debuginfo-7.0.7-55.1
php7-posix-7.0.7-55.1
php7-snmp-7.0.7-55.1
php7-phar-7.0.7-55.1
php7-bcmath-debuginfo-7.0.7-55.1
php7-fileinfo-7.0.7-55.1
php7-enchanted-7.0.7-55.1
apache2-mod_php7-7.0.7-55.1
php7-gmp-7.0.7-55.1
php7-ldap-debuginfo-7.0.7-55.1
php7-sysvmsg-debuginfo-7.0.7-55.1
php7-mysql-debuginfo-7.0.7-55.1
php7-mcrypt-7.0.7-55.1
php7-xmlrpc-7.0.7-55.1
php7-sysvmsg-7.0.7-55.1
php7-gettext-debuginfo-7.0.7-55.1
php7-wddx-7.0.7-55.1
php7-tidy-7.0.7-55.1
php7-xmlwriter-7.0.7-55.1
php7-tokenizer-7.0.7-55.1
php7-firebird-7.0.7-55.1
php7-imap-debuginfo-7.0.7-55.1
php7-curl-debuginfo-7.0.7-55.1
php7-ctype-debuginfo-7.0.7-55.1
apache2-mod_php7-debuginfo-7.0.7-55.1
php7-odbc-debuginfo-7.0.7-55.1
php7-pcntl-debuginfo-7.0.7-55.1
php7-posix-debuginfo-7.0.7-55.1
php7-xmlreader-debuginfo-7.0.7-55.1
php7-fastcgi-debuginfo-7.0.7-55.1
php7-pdo-7.0.7-55.1
php7-readline-7.0.7-55.1
php7-xmlreader-7.0.7-55.1
php7-dom-7.0.7-55.1
php7-opcache-7.0.7-55.1
php7-ftp-debuginfo-7.0.7-55.1
php7-json-debuginfo-7.0.7-55.1
php7-firebird-debuginfo-7.0.7-55.1
php7-xmlrpc-debuginfo-7.0.7-55.1
php7-ftp-7.0.7-55.1
php7-xsl-debuginfo-7.0.7-55.1

noarch

php7-pear-Archive_Tar-7.0.7-55.1
php7-pear-7.0.7-55.1

x86_64

php7-dba-7.0.7-55.1
php7-xsl-7.0.7-55.1
php7-intl-debuginfo-7.0.7-55.1
php7-calendar-debuginfo-7.0.7-55.1
php7-sysvshm-7.0.7-55.1
php7-tidy-debuginfo-7.0.7-55.1
php7-sqlite-debuginfo-7.0.7-55.1
php7-ldap-7.0.7-55.1
php7-iconv-7.0.7-55.1
php7-sockets-debuginfo-7.0.7-55.1
php7-pspell-7.0.7-55.1

php7-ctype-7.0.7-55.1
php7-dom-debuginfo-7.0.7-55.1
php7-pgsql-7.0.7-55.1
php7-mcrypt-debuginfo-7.0.7-55.1
php7-sysvsem-debuginfo-7.0.7-55.1
php7-zip-debuginfo-7.0.7-55.1
php7-sqlite-7.0.7-55.1
php7-bcmath-7.0.7-55.1
php7-devel-7.0.7-55.1
php7-zlib-debuginfo-7.0.7-55.1
php7-sockets-7.0.7-55.1
php7-bz2-debuginfo-7.0.7-55.1
php7-gmp-debuginfo-7.0.7-55.1
php7-openssl-7.0.7-55.1
php7-bz2-7.0.7-55.1
php7-mysql-7.0.7-55.1
php7-debuginfo-7.0.7-55.1
php7-curl-7.0.7-55.1
php7-exif-debuginfo-7.0.7-55.1
php7-fpm-debuginfo-7.0.7-55.1
php7-wddx-debuginfo-7.0.7-55.1
php7-phar-debuginfo-7.0.7-55.1
php7-odbc-7.0.7-55.1
php7-pgsql-debuginfo-7.0.7-55.1
php7-gettext-7.0.7-55.1
php7-shmop-debuginfo-7.0.7-55.1
php7-iconv-debuginfo-7.0.7-55.1
php7-gd-7.0.7-55.1
php7-pspell-debuginfo-7.0.7-55.1
php7-tokenizer-debuginfo-7.0.7-55.1
php7-mbstring-7.0.7-55.1
php7-exif-7.0.7-55.1
php7-calendar-7.0.7-55.1
php7-gd-debuginfo-7.0.7-55.1
php7-mbstring-debuginfo-7.0.7-55.1
php7-xmlwriter-debuginfo-7.0.7-55.1
php7-zlib-7.0.7-55.1
php7-dba-debuginfo-7.0.7-55.1
php7-debugsource-7.0.7-55.1
php7-pdo-debuginfo-7.0.7-55.1
php7-sysvshm-debuginfo-7.0.7-55.1
php7-sysvsem-7.0.7-55.1
php7-fpm-7.0.7-55.1
php7-ldap-7.0.7-55.1
php7-intl-7.0.7-55.1
php7-7.0.7-55.1
php7-json-7.0.7-55.1
php7-enchanted-debuginfo-7.0.7-55.1
php7-openssl-debuginfo-7.0.7-55.1
php7-zip-7.0.7-55.1
php7-shmop-7.0.7-55.1
php7-soap-7.0.7-55.1
php7-snmp-debuginfo-7.0.7-55.1
php7-pcntl-7.0.7-55.1
php7-soap-debuginfo-7.0.7-55.1
php7-readline-debuginfo-7.0.7-55.1
php7-fastcgi-7.0.7-55.1
php7-fileinfo-debuginfo-7.0.7-55.1
php7-opcache-debuginfo-7.0.7-55.1
php7-posix-7.0.7-55.1

php7-snmp-7.0.7-55.1
php7-phar-7.0.7-55.1
php7-bcmath-debuginfo-7.0.7-55.1
php7-fileinfo-7.0.7-55.1
php7-enchanted-7.0.7-55.1
apache2-mod_php7-7.0.7-55.1
php7-gmp-7.0.7-55.1
php7-ldap-debuginfo-7.0.7-55.1
php7-sysvmsg-debuginfo-7.0.7-55.1
php7-mysql-debuginfo-7.0.7-55.1
php7-mcrypt-7.0.7-55.1
php7-xmlrpc-7.0.7-55.1
php7-sysvmsg-7.0.7-55.1
php7-gettext-debuginfo-7.0.7-55.1
php7-wddx-7.0.7-55.1
php7-tidy-7.0.7-55.1
php7-xmlwriter-7.0.7-55.1
php7-tokenizer-7.0.7-55.1
php7-firebird-7.0.7-55.1
php7-imap-debuginfo-7.0.7-55.1
php7-curl-debuginfo-7.0.7-55.1
php7-ctype-debuginfo-7.0.7-55.1
apache2-mod_php7-debuginfo-7.0.7-55.1
php7-odbc-debuginfo-7.0.7-55.1
php7-pcntl-debuginfo-7.0.7-55.1
php7-posix-debuginfo-7.0.7-55.1
php7-xmlreader-debuginfo-7.0.7-55.1
php7-fastcgi-debuginfo-7.0.7-55.1
php7-pdo-7.0.7-55.1
php7-readline-7.0.7-55.1
php7-xmlreader-7.0.7-55.1
php7-dom-7.0.7-55.1
php7-opcache-7.0.7-55.1
php7-ftp-debuginfo-7.0.7-55.1
php7-json-debuginfo-7.0.7-55.1
php7-firebird-debuginfo-7.0.7-55.1
php7-xmlrpc-debuginfo-7.0.7-55.1
php7-ftp-7.0.7-55.1
php7-xsl-debuginfo-7.0.7-55.1

147641 - SuSE Linux 15.0 openSUSE-SU-2019:0189-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16873, CVE-2018-16874, CVE-2018-16875

Description

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

openSUSE-SU-2019:0189-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00078.html>

SuSE Linux 15.0

x86_64

containerd-1.1.2-lp150.4.6.1
docker-debuginfo-18.09.0_ce-lp150.5.9.1
docker-18.09.0_ce-lp150.5.9.1
docker-libnetwork-debuginfo-0.7.0.1+gitr2704_6da50d197830-lp150.3.6.1
docker-runc-1.0.0rc5+gitr3562_69663f0bd4b6-lp150.5.6.1
golang-github-docker-libnetwork-0.7.0.1+gitr2704_6da50d197830-lp150.3.6.1
docker-libnetwork-0.7.0.1+gitr2704_6da50d197830-lp150.3.6.1
docker-runc-debuginfo-1.0.0rc5+gitr3562_69663f0bd4b6-lp150.5.6.1
docker-debugsource-18.09.0_ce-lp150.5.9.1
containerd-ctr-1.1.2-lp150.4.6.1
docker-test-debuginfo-18.09.0_ce-lp150.5.9.1
docker-test-18.09.0_ce-lp150.5.9.1

noarch
docker-zsh-completion-18.09.0_ce-lp150.5.9.1
docker-bash-completion-18.09.0_ce-lp150.5.9.1
docker-runc-test-1.0.0rc5+gitr3562_69663f0bd4b6-lp150.5.6.1
containerd-test-1.1.2-lp150.4.6.1

147642 - SuSE SLES 11 SP4 SUSE-SU-2019:13961-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6977, CVE-2019-6978

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13961-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005123.html>

SuSE SLES 11 SP4

i586
php53-5.3.17-112.53.1
php53-dba-5.3.17-112.53.1
php53-pcntl-5.3.17-112.53.1
php53-pgsql-5.3.17-112.53.1
php53-ftp-5.3.17-112.53.1
php53-suhosin-5.3.17-112.53.1
php53-xmlrpc-5.3.17-112.53.1
php53-bz2-5.3.17-112.53.1
php53-sysvsem-5.3.17-112.53.1
php53-fastcgi-5.3.17-112.53.1
php53-fileinfo-5.3.17-112.53.1
apache2-mod_php53-5.3.17-112.53.1
php53-gmp-5.3.17-112.53.1
php53-ldap-5.3.17-112.53.1
php53-dom-5.3.17-112.53.1
php53-tokenizer-5.3.17-112.53.1
php53-sysvshm-5.3.17-112.53.1
php53-pspell-5.3.17-112.53.1
php53-soap-5.3.17-112.53.1
php53-openssl-5.3.17-112.53.1
php53-mysql-5.3.17-112.53.1

php53-zlib-5.3.17-112.53.1
php53-sysvmsg-5.3.17-112.53.1
php53-xsl-5.3.17-112.53.1
php53-pear-5.3.17-112.53.1
php53-shmop-5.3.17-112.53.1
php53-ctype-5.3.17-112.53.1
php53-wddx-5.3.17-112.53.1
php53-gettext-5.3.17-112.53.1
php53-snmp-5.3.17-112.53.1
php53-odbc-5.3.17-112.53.1
php53-curl-5.3.17-112.53.1
php53-json-5.3.17-112.53.1
php53-xmlreader-5.3.17-112.53.1
php53-calendar-5.3.17-112.53.1
php53-zip-5.3.17-112.53.1
php53-iconv-5.3.17-112.53.1
php53-xmlwriter-5.3.17-112.53.1
php53-bcmath-5.3.17-112.53.1
php53-exif-5.3.17-112.53.1
php53-mbstring-5.3.17-112.53.1
php53-intl-5.3.17-112.53.1
php53-mcrypt-5.3.17-112.53.1
php53-pdo-5.3.17-112.53.1
php53-gd-5.3.17-112.53.1

x86_64

php53-5.3.17-112.53.1
php53-dba-5.3.17-112.53.1
php53-pcntl-5.3.17-112.53.1
php53-pgsql-5.3.17-112.53.1
php53-ftp-5.3.17-112.53.1
php53-suhosin-5.3.17-112.53.1
php53-xmlrpc-5.3.17-112.53.1
php53-bz2-5.3.17-112.53.1
php53-sysvsem-5.3.17-112.53.1
php53-fastcgi-5.3.17-112.53.1
php53-fileinfo-5.3.17-112.53.1
apache2-mod_php53-5.3.17-112.53.1
php53-gmp-5.3.17-112.53.1
php53-ldap-5.3.17-112.53.1
php53-dom-5.3.17-112.53.1
php53-tokenizer-5.3.17-112.53.1
php53-sysvshm-5.3.17-112.53.1
php53-pspell-5.3.17-112.53.1
php53-soap-5.3.17-112.53.1
php53-openssl-5.3.17-112.53.1
php53-mysql-5.3.17-112.53.1
php53-zlib-5.3.17-112.53.1
php53-sysvmsg-5.3.17-112.53.1
php53-xsl-5.3.17-112.53.1
php53-pear-5.3.17-112.53.1
php53-shmop-5.3.17-112.53.1
php53-ctype-5.3.17-112.53.1
php53-wddx-5.3.17-112.53.1
php53-gettext-5.3.17-112.53.1
php53-snmp-5.3.17-112.53.1
php53-odbc-5.3.17-112.53.1
php53-curl-5.3.17-112.53.1
php53-json-5.3.17-112.53.1
php53-xmlreader-5.3.17-112.53.1

php53-calendar-5.3.17-112.53.1
php53-zip-5.3.17-112.53.1
php53-iconv-5.3.17-112.53.1
php53-xmlwriter-5.3.17-112.53.1
php53-bcmath-5.3.17-112.53.1
php53-exif-5.3.17-112.53.1
php53-mbstring-5.3.17-112.53.1
php53-intl-5.3.17-112.53.1
php53-mcrypt-5.3.17-112.53.1
php53-pdo-5.3.17-112.53.1
php53-gd-5.3.17-112.53.1

147644 - SuSE Linux 42.3 openSUSE-SU-2019:0200-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20748, CVE-2018-20749, CVE-2018-20750

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0200-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00092.html>

SuSE Linux 42.3

x86_64

libvncclient0-0.9.9-16.9.1

LibVNCServer-debugsource-0.9.9-16.9.1

linuxvnc-0.9.9-16.9.1

libvncclient0-debuginfo-0.9.9-16.9.1

libvncserver0-0.9.9-16.9.1

libvncserver0-debuginfo-0.9.9-16.9.1

LibVNCServer-devel-0.9.9-16.9.1

linuxvnc-debuginfo-0.9.9-16.9.1

i586

libvncclient0-0.9.9-16.9.1

LibVNCServer-debugsource-0.9.9-16.9.1

linuxvnc-0.9.9-16.9.1

libvncclient0-debuginfo-0.9.9-16.9.1

libvncserver0-0.9.9-16.9.1

libvncserver0-debuginfo-0.9.9-16.9.1

LibVNCServer-devel-0.9.9-16.9.1

linuxvnc-debuginfo-0.9.9-16.9.1

147649 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0428-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0428-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005135.html>

SuSE SLED 12 SP3

x86_64
systemd-debugsource-228-150.63.1
systemd-debuginfo-32bit-228-150.63.1
systemd-32bit-228-150.63.1
udev-debuginfo-228-150.63.1
libudev1-32bit-228-150.63.1
libsystemd0-32bit-228-150.63.1
libsystemd0-debuginfo-32bit-228-150.63.1
libudev1-228-150.63.1
systemd-debuginfo-228-150.63.1
libudev1-debuginfo-32bit-228-150.63.1
systemd-228-150.63.1
libsystemd0-228-150.63.1
libudev1-debuginfo-228-150.63.1
udev-228-150.63.1
systemd-sysvinit-228-150.63.1
libsystemd0-debuginfo-228-150.63.1

noarch
systemd-bash-completion-228-150.63.1

SuSE SLED 12 SP4

x86_64
systemd-debugsource-228-150.63.1
systemd-debuginfo-32bit-228-150.63.1
systemd-32bit-228-150.63.1
udev-debuginfo-228-150.63.1
libudev1-32bit-228-150.63.1
libsystemd0-32bit-228-150.63.1
libsystemd0-debuginfo-32bit-228-150.63.1
libudev1-228-150.63.1
systemd-debuginfo-228-150.63.1
libudev1-debuginfo-32bit-228-150.63.1
systemd-228-150.63.1
libsystemd0-228-150.63.1
libudev1-debuginfo-228-150.63.1
udev-228-150.63.1
systemd-sysvinit-228-150.63.1
libsystemd0-debuginfo-228-150.63.1

noarch
systemd-bash-completion-228-150.63.1

SuSE SLES 12 SP4

noarch
systemd-bash-completion-228-150.63.1

x86_64
systemd-debuginfo-32bit-228-150.63.1
systemd-32bit-228-150.63.1

udev-debuginfo-228-150.63.1
libudev1-32bit-228-150.63.1
systemd-debugsource-228-150.63.1
libsystemd0-debuginfo-32bit-228-150.63.1
libudev1-228-150.63.1
systemd-debuginfo-228-150.63.1
libudev1-debuginfo-32bit-228-150.63.1
systemd-228-150.63.1
libsystemd0-228-150.63.1
libudev1-debuginfo-228-150.63.1
udev-228-150.63.1
systemd-sysvinit-228-150.63.1
libsystemd0-32bit-228-150.63.1
libsystemd0-debuginfo-228-150.63.1

SuSE SLES 12 SP3

noarch
systemd-bash-completion-228-150.63.1

x86_64

systemd-debuginfo-32bit-228-150.63.1
systemd-32bit-228-150.63.1
udev-debuginfo-228-150.63.1
libudev1-32bit-228-150.63.1
systemd-debugsource-228-150.63.1
libsystemd0-debuginfo-32bit-228-150.63.1
libudev1-228-150.63.1
systemd-debuginfo-228-150.63.1
libudev1-debuginfo-32bit-228-150.63.1
systemd-228-150.63.1
libsystemd0-228-150.63.1
libudev1-debuginfo-228-150.63.1
udev-228-150.63.1
systemd-sysvinit-228-150.63.1
libsystemd0-32bit-228-150.63.1
libsystemd0-debuginfo-228-150.63.1

147652 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0195-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16843, CVE-2018-16844, CVE-2018-16845

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0195-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00090.html>

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00088.html>

SuSE Linux 15.0

x86_64

nginx-debuginfo-1.14.2-lp150.2.4.1

vim-plugin-nginx-1.14.2-16.1

nginx-debugsource-1.14.2-lp150.2.4.1
nginx-1.14.2-lp150.2.4.1

noarch
vim-plugin-nginx-1.14.2-lp150.2.4.1

SuSE Linux 42.3
i586
nginx-debugsource-1.14.2-2.7.1
nginx-1.14.2-2.7.1
nginx-debuginfo-1.14.2-2.7.1

noarch
vim-plugin-nginx-1.14.2-2.7.1

x86_64
nginx-debugsource-1.14.2-2.7.1
nginx-1.14.2-2.7.1
nginx-debuginfo-1.14.2-2.7.1

147654 - SuSE Linux 42.3 openSUSE-SU-2019:0173-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0173-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00061.html>

SuSE Linux 42.3
x86_64
curl-7.37.0-45.1
libcurl4-7.37.0-45.1
libcurl-devel-32bit-7.37.0-45.1
libcurl4-debuginfo-7.37.0-45.1
curl-debuginfo-7.37.0-45.1
curl-debugsource-7.37.0-45.1
libcurl4-debuginfo-32bit-7.37.0-45.1
libcurl4-32bit-7.37.0-45.1
libcurl-devel-7.37.0-45.1

i586
curl-7.37.0-45.1
libcurl4-7.37.0-45.1
libcurl4-debuginfo-7.37.0-45.1
curl-debuginfo-7.37.0-45.1
curl-debugsource-7.37.0-45.1
libcurl-devel-7.37.0-45.1

147655 - SuSE Linux 15.0 openSUSE-SU-2019:0183-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12404

Description

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

openSUSE-SU-2019:0183-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00072.html>

SuSE Linux 15.0

x86_64

mozilla-nss-sysinit-debuginfo-3.41.1-lp150.2.16.1

libfreebl3-debuginfo-3.41.1-lp150.2.16.1

libfreebl3-3.41.1-lp150.2.16.1

mozilla-nss-32bit-3.41.1-lp150.2.16.1

libsoftokn3-32bit-3.41.1-lp150.2.16.1

mozilla-nss-certs-32bit-3.41.1-lp150.2.16.1

libsoftokn3-hmac-3.41.1-lp150.2.16.1

mozilla-nss-certs-32bit-debuginfo-3.41.1-lp150.2.16.1

libfreebl3-hmac-32bit-3.41.1-lp150.2.16.1

mozilla-nss-sysinit-32bit-3.41.1-lp150.2.16.1

libsoftokn3-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-sysinit-32bit-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-sysinit-3.41.1-lp150.2.16.1

libfreebl3-32bit-3.41.1-lp150.2.16.1

libfreebl3-hmac-3.41.1-lp150.2.16.1

mozilla-nss-debugsource-3.41.1-lp150.2.16.1

mozilla-nss-3.41.1-lp150.2.16.1

mozilla-nss-certs-3.41.1-lp150.2.16.1

mozilla-nss-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-tools-debuginfo-3.41.1-lp150.2.16.1

libsoftokn3-32bit-debuginfo-3.41.1-lp150.2.16.1

libsoftokn3-hmac-32bit-3.41.1-lp150.2.16.1

libsoftokn3-3.41.1-lp150.2.16.1

libfreebl3-32bit-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-32bit-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-devel-3.41.1-lp150.2.16.1

mozilla-nss-tools-3.41.1-lp150.2.16.1

mozilla-nss-certs-debuginfo-3.41.1-lp150.2.16.1

i586

libfreebl3-3.41.1-lp150.2.16.1

mozilla-nss-sysinit-3.41.1-lp150.2.16.1

libsoftokn3-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-debugsource-3.41.1-lp150.2.16.1

mozilla-nss-3.41.1-lp150.2.16.1

mozilla-nss-tools-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-certs-3.41.1-lp150.2.16.1

mozilla-nss-devel-3.41.1-lp150.2.16.1

mozilla-nss-debuginfo-3.41.1-lp150.2.16.1

libfreebl3-hmac-3.41.1-lp150.2.16.1

libsoftokn3-hmac-3.41.1-lp150.2.16.1

mozilla-nss-certs-debuginfo-3.41.1-lp150.2.16.1

mozilla-nss-tools-3.41.1-lp150.2.16.1

libsoftokn3-3.41.1-lp150.2.16.1
libfreebl3-debuginfo-3.41.1-lp150.2.16.1
mozilla-nss-sysinit-debuginfo-3.41.1-lp150.2.16.1

147656 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0194-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6798, CVE-2019-6799

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0194-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00089.html>

SuSE Linux 15.0
noarch
phpMyAdmin-4.8.5-lp150.2.15.1

SuSE Linux 42.3
noarch
phpMyAdmin-4.8.5-27.1

147657 - SuSE Linux 15.0 openSUSE-SU-2019:0165-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19198, CVE-2018-19199, CVE-2018-19200, CVE-2018-20721

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0165-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00053.html>

SuSE Linux 15.0
x86_64
liburiparser1-32bit-debuginfo-0.8.5-lp150.2.3.1
uriparser-debuginfo-0.8.5-lp150.2.3.1
liburiparser1-debuginfo-0.8.5-lp150.2.3.1
liburiparser1-32bit-0.8.5-lp150.2.3.1
uriparser-devel-0.8.5-lp150.2.3.1
uriparser-debugsource-0.8.5-lp150.2.3.1
liburiparser1-0.8.5-lp150.2.3.1
uriparser-0.8.5-lp150.2.3.1

i586

uriparser-debuginfo-0.8.5-lp150.2.3.1
liburiparser1-debuginfo-0.8.5-lp150.2.3.1
uriparser-devel-0.8.5-lp150.2.3.1
uriparser-debugsource-0.8.5-lp150.2.3.1
liburiparser1-0.8.5-lp150.2.3.1
uriparser-0.8.5-lp150.2.3.1

147660 - SuSE Linux 15.0 openSUSE-SU-2019:0197-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000845

Description

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

openSUSE-SU-2019:0197-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00086.html>

SuSE Linux 15.0

i586

libavahi-client3-0.6.32-lp150.4.3.1
libavahi-glib1-0.6.32-lp150.4.3.1
libavahi-common3-0.6.32-lp150.4.3.1
libavahi-gobject-devel-0.6.32-lp150.4.3.1
avahi-glib2-debugsource-0.6.32-lp150.4.3.1
typelib-1_0-Avahi-0_6-0.6.32-lp150.4.3.1
avahi-autoipd-0.6.32-lp150.4.3.1
avahi-compatible-mDNSResponder-devel-0.6.32-lp150.4.3.1
avahi-utils-0.6.32-lp150.4.3.1
libavahi-ui0-0.6.32-lp150.4.3.1
avahi-debugsource-0.6.32-lp150.4.3.1
libavahi-client3-debuginfo-0.6.32-lp150.4.3.1
libdns_sd-0.6.32-lp150.4.3.1
avahi-utils-gtk-debuginfo-0.6.32-lp150.4.3.1
avahi-compatible-howl-devel-0.6.32-lp150.4.3.1
avahi-debuginfo-0.6.32-lp150.4.3.1
libdns_sd-debuginfo-0.6.32-lp150.4.3.1
libavahi-glib1-debuginfo-0.6.32-lp150.4.3.1
libhowl0-debuginfo-0.6.32-lp150.4.3.1
libavahi-ui0-debuginfo-0.6.32-lp150.4.3.1
libavahi-glib-devel-0.6.32-lp150.4.3.1
libavahi-common3-debuginfo-0.6.32-lp150.4.3.1
python-avahi-gtk-0.6.32-lp150.4.3.1
libavahi-ui-gtk3-0-0.6.32-lp150.4.3.1
libhowl0-0.6.32-lp150.4.3.1
avahi-0.6.32-lp150.4.3.1
avahi-utils-gtk-0.6.32-lp150.4.3.1
libavahi-devel-0.6.32-lp150.4.3.1
libavahi-core7-0.6.32-lp150.4.3.1
libavahi-core7-debuginfo-0.6.32-lp150.4.3.1
libavahi-ui-gtk3-0-debuginfo-0.6.32-lp150.4.3.1
libavahi-gobject0-0.6.32-lp150.4.3.1
python-avahi-0.6.32-lp150.4.3.1

avahi-utils-debuginfo-0.6.32-lp150.4.3.1
libavahi-gobject0-debuginfo-0.6.32-lp150.4.3.1
avahi-autoipd-debuginfo-0.6.32-lp150.4.3.1

noarch
avahi-lang-0.6.32-lp150.4.3.1

x86_64
libavahi-client3-0.6.32-lp150.4.3.1
libavahi-common3-32bit-debuginfo-0.6.32-lp150.4.3.1
libavahi-glib1-0.6.32-lp150.4.3.1
libavahi-common3-0.6.32-lp150.4.3.1
libavahi-gobject-devel-0.6.32-lp150.4.3.1
avahi-32bit-debuginfo-0.6.32-lp150.4.3.1
avahi-glib2-debugsource-0.6.32-lp150.4.3.1
libavahi-qt4-devel-0.6.32-lp150.4.3.1
libavahi-qt4-1-0.6.32-lp150.4.3.1
typelib-1_0-Avahi-0_6-0.6.32-lp150.4.3.1
avahi-autoipd-0.6.32-lp150.4.3.1
avahi-compat-mDNSResponder-devel-0.6.32-lp150.4.3.1
avahi-utils-0.6.32-lp150.4.3.1
libavahi-ui0-0.6.32-lp150.4.3.1
avahi-debugsource-0.6.32-lp150.4.3.1
libavahi-client3-debuginfo-0.6.32-lp150.4.3.1
libdns_sd-0.6.32-lp150.4.3.1
avahi-utils-gtk-debuginfo-0.6.32-lp150.4.3.1
avahi-compat-howl-devel-0.6.32-lp150.4.3.1
avahi-debuginfo-0.6.32-lp150.4.3.1
libdns_sd-debuginfo-0.6.32-lp150.4.3.1
libavahi-glib1-debuginfo-0.6.32-lp150.4.3.1
libhowl0-debuginfo-0.6.32-lp150.4.3.1
libavahi-ui0-debuginfo-0.6.32-lp150.4.3.1
libavahi-qt4-1-debuginfo-0.6.32-lp150.4.3.1
avahi-qt4-debugsource-0.6.32-lp150.4.3.1
libdns_sd-32bit-0.6.32-lp150.4.3.1
libdns_sd-32bit-debuginfo-0.6.32-lp150.4.3.1
libavahi-glib-devel-0.6.32-lp150.4.3.1
libavahi-common3-debuginfo-0.6.32-lp150.4.3.1
libavahi-common3-32bit-0.6.32-lp150.4.3.1
libavahi-glib1-32bit-debuginfo-0.6.32-lp150.4.3.1
python-avahi-gtk-0.6.32-lp150.4.3.1
libavahi-ui-gtk3-0-0.6.32-lp150.4.3.1
libavahi-client3-32bit-debuginfo-0.6.32-lp150.4.3.1
libhowl0-0.6.32-lp150.4.3.1
avahi-0.6.32-lp150.4.3.1
libavahi-glib1-32bit-0.6.32-lp150.4.3.1
avahi-utils-gtk-0.6.32-lp150.4.3.1
avahi-mono-0.6.32-lp150.4.3.1
libavahi-devel-0.6.32-lp150.4.3.1
libavahi-core7-0.6.32-lp150.4.3.1
libavahi-core7-debuginfo-0.6.32-lp150.4.3.1
libavahi-client3-32bit-0.6.32-lp150.4.3.1
libavahi-ui-gtk3-0-debuginfo-0.6.32-lp150.4.3.1
libavahi-gobject0-0.6.32-lp150.4.3.1
python-avahi-0.6.32-lp150.4.3.1
avahi-utils-debuginfo-0.6.32-lp150.4.3.1
libavahi-gobject0-debuginfo-0.6.32-lp150.4.3.1
avahi-autoipd-debuginfo-0.6.32-lp150.4.3.1

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

Risk Level: High

CVE: CVE-2019-6454

Description

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

ELSA-2019-0368

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2019-February/008492.html>

OEL7

x86_64

systemd-libs-219-62.0.4.el7_6.5

systemd-sysv-219-62.0.4.el7_6.5

systemd-resolved-219-62.0.4.el7_6.5

libgudev1-devel-219-62.0.4.el7_6.5

systemd-devel-219-62.0.4.el7_6.5

systemd-networkd-219-62.0.4.el7_6.5

systemd-219-62.0.4.el7_6.5

systemd-python-219-62.0.4.el7_6.5

libgudev1-219-62.0.4.el7_6.5

systemd-journal-gateway-219-62.0.4.el7_6.5

194774 - Fedora Linux 28 FEDORA-2019-5146cd34e2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20174, CVE-2018-20175, CVE-2018-20176, CVE-2018-20177, CVE-2018-20178, CVE-2018-20179, CVE-2018-20180, CVE-2018-20181, CVE-2018-20182, CVE-2018-8791, CVE-2018-8792, CVE-2018-8793, CVE-2018-8794, CVE-2018-8795, CVE-2018-8796, CVE-2018-8797, CVE-2018-8798, CVE-2018-8799, CVE-2018-8800

Description

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

FEDORA-2019-5146cd34e2

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/2019/2/?count=200&page=2>

Fedora Core 28

rdesktop-1.8.4-2.fc28

194784 - Fedora Linux 29 FEDORA-2019-164946aa7f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16862, CVE-2018-16880, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222

Description

The scan detected that the host is missing the following update:
FEDORA-2019-164946aa7f

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/2019/2/?count=200&page=1>

Fedora Core 29

kernel-tools-4.20.8-200.fc29
kernel-headers-4.20.8-200.fc29
kernel-4.20.8-200.fc29

194790 - Fedora Linux 29 FEDORA-2019-e2f47b40a3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20030

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e2f47b40a3

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/2019/2/?count=200&page=2>

Fedora Core 29

libexif-0.6.21-19.fc29

194796 - Fedora Linux 28 FEDORA-2019-82acb29c1b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10194, CVE-2018-16802, CVE-2018-17183, CVE-2018-17961, CVE-2018-18073, CVE-2018-18284, CVE-2018-19134, CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477, CVE-2018-19478

Description

The scan detected that the host is missing the following update:
FEDORA-2019-82acb29c1b

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/2019/2/?count=200&page=1>

Fedora Core 28

ghostscript-9.26-1.fc28

194801 - Fedora Linux 29 FEDORA-2019-df57551f6d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7051, CVE-2018-1000873, CVE-2018-12022, CVE-2018-12023, CVE-2018-14718, CVE-2018-147189, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361, CVE-2018-19362

Description

The scan detected that the host is missing the following update:
FEDORA-2019-df57551f6d

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/2019/2/?count=200&page=1>

Fedora Core 29

jackson-dataformats-text-2.9.8-1.fc29
jackson-dataformats-binary-2.9.8-1.fc29
jackson-bom-2.9.8-1.fc29
eclipse-jgit-5.2.0-4.fc29
jackson-modules-base-2.9.8-1.fc29
jackson-core-2.9.8-1.fc29
jackson-parent-2.9.1.2-1.fc29
jackson-datatype-jdk8-2.9.8-1.fc29
jackson-module-jsonSchema-2.9.8-1.fc29
jackson-annotations-2.9.8-1.fc29
jackson-datatype-joda-2.9.8-1.fc29
eclipse-linuxtools-7.1.0-3.fc29
jackson-jaxrs-providers-2.9.8-1.fc29
jackson-dataformat-xml-2.9.8-1.fc29
jackson-databind-2.9.8-1.fc29
bouncycastle-1.61-1.fc29
jackson-datatypes-collections-2.9.8-1.fc29

196253 - Red Hat Enterprise Linux RHSA-2019-0368 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
RHSA-2019-0368

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-February/msg00020.html>

RHEL7D
x86_64
libgudev1-devel-219-62.el7_6.5
systemd-sysv-219-62.el7_6.5
systemd-libs-219-62.el7_6.5
systemd-networkd-219-62.el7_6.5
systemd-devel-219-62.el7_6.5
libgudev1-219-62.el7_6.5
systemd-219-62.el7_6.5
systemd-python-219-62.el7_6.5
systemd-debuginfo-219-62.el7_6.5
systemd-resolved-219-62.el7_6.5
systemd-journal-gateway-219-62.el7_6.5

RHEL7S
x86_64
libgudev1-devel-219-62.el7_6.5
systemd-sysv-219-62.el7_6.5
systemd-libs-219-62.el7_6.5
systemd-networkd-219-62.el7_6.5
systemd-devel-219-62.el7_6.5
libgudev1-219-62.el7_6.5
systemd-219-62.el7_6.5
systemd-python-219-62.el7_6.5
systemd-debuginfo-219-62.el7_6.5
systemd-resolved-219-62.el7_6.5
systemd-journal-gateway-219-62.el7_6.5

RHEL7WS
x86_64
libgudev1-devel-219-62.el7_6.5
systemd-sysv-219-62.el7_6.5
systemd-libs-219-62.el7_6.5
systemd-networkd-219-62.el7_6.5
systemd-devel-219-62.el7_6.5
libgudev1-219-62.el7_6.5
systemd-219-62.el7_6.5
systemd-python-219-62.el7_6.5
systemd-debuginfo-219-62.el7_6.5
systemd-resolved-219-62.el7_6.5
systemd-journal-gateway-219-62.el7_6.5

196254 - Red Hat Enterprise Linux RHSA-2019-0348 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7090

Description

The scan detected that the host is missing the following update:
RHSA-2019-0348

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-February/msg00012.html>

RHEL6D
x86_64
flash-plugin-32.0.0.142-1.el6_10

i386
flash-plugin-32.0.0.142-1.el6_10

RHEL6S
x86_64
flash-plugin-32.0.0.142-1.el6_10

i386
flash-plugin-32.0.0.142-1.el6_10

RHEL6WS
x86_64
flash-plugin-32.0.0.142-1.el6_10

i386
flash-plugin-32.0.0.142-1.el6_10

24760 - (HT209450) Apple iTunes Vulnerabilities Prior To 12.9.3

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

Risk Level: Medium

CVE: CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6221, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234, CVE-2019-6235

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code or cause a cross site scripting attack on the target system.

24771 - IBM Tivoli Storage Manager FastBack Java Runtime Vulnerabilities (ibm10793819)

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

Risk Level: Medium

CVE: CVE-2018-3139, CVE-2018-3180

Description

Multiple vulnerabilities are present in some versions of IBM Tivoli Storage Manager FastBack.

Observation

IBM Tivoli Storage Manager FastBack is a data protection and recovery software.

Multiple vulnerabilities are present in some versions of IBM Tivoli Storage Manager FastBack. The flaws lie in the JRE component. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service condition on the target system.

89004 - Slackware Linux 14.2 SSA:2019-045-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2018-18509, CVE-2019-5785

Description

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

SSA:2019-045-01

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=2019&m=slackware-security.396014>

Slackware 14.2

x86_64

mozilla-thunderbird-60.5.1-x86_64-1

i686

mozilla-thunderbird-60.5.1-i686-1

89005 - Slackware Linux 14.2 SSA:2019-044-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2019-5785

Description

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

SSA:2019-044-01

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=2019&m=slackware-security.380697>

Slackware 14.2

x86_64

mozilla-firefox-60.5.1esr-x86_64-1

i686

mozilla-firefox-60.5.1esr-i686-1

131301 - Debian Linux 9.0 DSA-4391-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

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

DSA-4391-1

Observation

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

<http://www.debian.org/security/2019/dsa-4391>

Debian 9.0

all

firefox-esr_60.5.1esr-1~deb9u1

147636 - SuSE Linux 15.0 openSUSE-SU-2019:0198-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20230

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0198-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00084.html>

SuSE Linux 15.0

x86_64

pspp-1.2.0-lp150.2.3.1

libspread-sheet-widget0-0.3-lp150.2.1

spread-sheet-widget-devel-0.3-lp150.2.1

spread-sheet-widget-debugsource-0.3-lp150.2.1

pspp-debuginfo-1.2.0-lp150.2.3.1

pspp-devel-1.2.0-lp150.2.3.1

libspread-sheet-widget0-debuginfo-0.3-lp150.2.1

pspp-debugsource-1.2.0-lp150.2.3.1

147638 - SuSE Linux 42.3 openSUSE-SU-2019:0202-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0202-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00091.html>

SuSE Linux 42.3
x86_64
MozillaFirefox-translations-common-60.5.1-131.1
MozillaFirefox-debuginfo-60.5.1-131.1
MozillaFirefox-branding-upstream-60.5.1-131.1
MozillaFirefox-buildsymbols-60.5.1-131.1
MozillaFirefox-devel-60.5.1-131.1
MozillaFirefox-translations-other-60.5.1-131.1
MozillaFirefox-debugsource-60.5.1-131.1
MozillaFirefox-60.5.1-131.1

147643 - SuSE Linux 42.3 openSUSE-SU-2019:0212-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20230

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0212-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00105.html>

SuSE Linux 42.3
x86_64
spread-sheet-widget-debugsource-0.3-2.1
pspp-debuginfo-1.2.0-11.1
libspread-sheet-widget0-0.3-2.1
pspp-debugsource-1.2.0-11.1
pspp-devel-1.2.0-11.1
spread-sheet-widget-devel-0.3-2.1
libspread-sheet-widget0-debuginfo-0.3-2.1
pspp-1.2.0-11.1

i586
libspread-sheet-widget0-debuginfo-0.3-2.1
libspread-sheet-widget0-0.3-2.1
spread-sheet-widget-debugsource-0.3-2.1
spread-sheet-widget-devel-0.3-2.1

147645 - SuSE Linux 42.3 openSUSE-SU-2019:0205-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782, CVE-2019-5784

Description

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

openSUSE-SU-2019:0205-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00097.html>

SuSE Linux 42.3
x86_64
chromedriver-debuginfo-72.0.3626.96-197.1
chromedriver-72.0.3626.96-197.1
chromium-debugsource-72.0.3626.96-197.1
chromium-72.0.3626.96-197.1
chromium-debuginfo-72.0.3626.96-197.1

147648 - SuSE Linux 15.0 openSUSE-SU-2019:0204-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782, CVE-2019-5784

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0204-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00095.html>

SuSE Linux 15.0
x86_64
chromium-debugsource-72.0.3626.96-lp150.2.41.1
chromium-72.0.3626.96-lp150.2.41.1
chromium-debuginfo-72.0.3626.96-lp150.2.41.1
chromedriver-debuginfo-72.0.3626.96-lp150.2.41.1
chromedriver-72.0.3626.96-lp150.2.41.1

147659 - SuSE SLED 12 SP3, 12 SP4 SUSE-SU-2019:0393-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6845, CVE-2017-7381, CVE-2017-7382, CVE-2017-7383, CVE-2017-8054, CVE-2018-11256, CVE-2018-5295, CVE-2018-5296, CVE-2018-5308, CVE-2018-5309, CVE-2018-5783

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0393-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005117.html>

SuSE SLED 12 SP4

x86_64
libpodof0_9_2-0.9.2-3.6.3
libpodof0_9_2-debuginfo-0.9.2-3.6.3
podof0-debuginfo-0.9.2-3.6.3
podof0-debugsource-0.9.2-3.6.3

SuSE SLED 12 SP3

x86_64
libpodof0_9_2-0.9.2-3.6.3
libpodof0_9_2-debuginfo-0.9.2-3.6.3
podof0-debuginfo-0.9.2-3.6.3
podof0-debugsource-0.9.2-3.6.3

163807 - Oracle Enterprise Linux ELSA-2019-0373 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
ELSA-2019-0373

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-February/008493.html>

OEL6
x86_64
firefox-60.5.1-1.0.1.el6_10

163809 - Oracle Enterprise Linux ELSA-2019-0374 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
ELSA-2019-0374

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-February/008491.html>

OEL7
x86_64
firefox-60.5.1-1.0.1.el7_6

182915 - FreeBSD mozilla Multiple Vulnerabilities (18211552-f650-4d86-ba4f-e6d5cbfcdbeb)

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2018-18511, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (18211552-f650-4d86-ba4f-e6d5cbfcdbeb)

Observation

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

<http://www.vuxml.org/freebsd/18211552-f650-4d86-ba4f-e6d5cbfcdbeb.html>

Affected packages:

firefox < 65.0.1,1
firefox-esr < 60.5.1,1
thunderbird < 60.5.1

194776 - Fedora Linux 28 FEDORA-2019-7696bb57ca Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10851, CVE-2018-14626, CVE-2018-14644, CVE-2018-16855, CVE-2019-3806, CVE-2019-3807

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7696bb57ca

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/2019/2/?count=200&page=2>

Fedora Core 28

pdns-recursor-4.1.9-1.fc28

194785 - Fedora Linux 29 FEDORA-2019-c83703be82 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10779, CVE-2018-17100, CVE-2018-17101, CVE-2019-6128, CVE-2019-7663

Description

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

FEDORA-2019-c83703be82

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/2019/2/?count=200&page=1>

Fedora Core 29

libtiff-4.0.10-4.fc29

194787 - Fedora Linux 29 FEDORA-2019-6cc827b7a1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11254, CVE-2018-11255, CVE-2018-11256, CVE-2018-12982, CVE-2018-14320, CVE-2018-19532, CVE-2018-20751, CVE-2018-5783

Description

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

FEDORA-2019-6cc827b7a1

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/2019/2/?count=200&page=1>

Fedora Core 29

mingw-podofo-0.9.6-7.fc29

podofo-0.9.6-5.fc29

196250 - Red Hat Enterprise Linux RHSA-2019-0373 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

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

RHSA-2019-0373

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-February/msg00022.html>

RHEL6D

x86_64

firefox-60.5.1-1.el6_10

firefox-debuginfo-60.5.1-1.el6_10

i386
firefox-60.5.1-1.el6_10
firefox-debuginfo-60.5.1-1.el6_10

RHEL6S
i386
firefox-60.5.1-1.el6_10
firefox-debuginfo-60.5.1-1.el6_10

x86_64
firefox-60.5.1-1.el6_10
firefox-debuginfo-60.5.1-1.el6_10

RHEL6WS
x86_64
firefox-60.5.1-1.el6_10
firefox-debuginfo-60.5.1-1.el6_10

i386
firefox-60.5.1-1.el6_10
firefox-debuginfo-60.5.1-1.el6_10

196251 - Red Hat Enterprise Linux RHSA-2019-0374 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
RHSA-2019-0374

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-February/msg00023.html>

RHEL7D
x86_64
firefox-debuginfo-60.5.1-1.el7_6
firefox-60.5.1-1.el7_6

RHEL7S
x86_64
firefox-debuginfo-60.5.1-1.el7_6
firefox-60.5.1-1.el7_6

RHEL7WS
x86_64
firefox-debuginfo-60.5.1-1.el7_6
firefox-60.5.1-1.el7_6

24679 - (CTX240139) Citrix NetScaler ADC TLS Padding Oracle Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-6485

Description

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

Observation

Citrix NetScaler is a widely used product that helps enterprises to protect, control and improve their services.

A vulnerability is present in some versions of Citrix NetScaler Gateway. The flaw lies in the Citrix Application Delivery Controller, that's using hardware acceleration. Successful exploitation could allow an attacker to decrypt TLS traffic.

24726 - Cisco IOS Software Secure Shell Connection on VRF Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-0484

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in the SSH module. Successful exploitation could allow an attacker to affect the integrity of the target system.

24770 - Oracle HTTP Server Critical Patch Update January 2019

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

Risk Level: Medium

CVE: CVE-2019-2414

Description

A vulnerability is present in some versions of Oracle HTTP Server.

Observation

Oracle HTTP Server is a web server based on the Apache HTTP Server

A vulnerability is present in some versions of Oracle HTTP Server. The flaw lies in the Web Listener component. Successful exploitation could allow an attacker to affect the integrity, confidentiality, and availability of the target system.

24775 - (JSA10905) Juniper Junos OS EX and QFX Series Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0005

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in the Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in Junos firewall filter configuration component. Successful exploitation could allow an attacker to bypass certain security restrictions and perform unauthorized actions on the system.

147625 - SuSE Linux 15.0 openSUSE-SU-2019:0175-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6706

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0175-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00066.html>

SuSE Linux 15.0

i586

lua53-debuginfo-5.3.4-lp150.2.3.1

lua53-debugsource-5.3.4-lp150.2.3.1

lua53-devel-5.3.4-lp150.2.3.1

liblua5_3-5-5.3.4-lp150.2.3.1

liblua5_3-5-debuginfo-5.3.4-lp150.2.3.1

lua53-5.3.4-lp150.2.3.1

noarch

lua53-doc-5.3.4-lp150.2.3.1

x86_64

lua53-debuginfo-5.3.4-lp150.2.3.1

lua53-debugsource-5.3.4-lp150.2.3.1

lua53-devel-5.3.4-lp150.2.3.1

liblua5_3-5-32bit-debuginfo-5.3.4-lp150.2.3.1

liblua5_3-5-5.3.4-lp150.2.3.1

liblua5_3-5-debuginfo-5.3.4-lp150.2.3.1

liblua5_3-5-32bit-5.3.4-lp150.2.3.1

lua53-5.3.4-lp150.2.3.1

147626 - SuSE Linux 15.0 openSUSE-SU-2019:0185-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14404, CVE-2018-16468, CVE-2018-16470

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0185-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00070.html>

SuSE Linux 15.0

x86_64

rmt-server-1.1.1-lp150.2.12.1

rmt-server-pubcloud-1.1.1-lp150.2.12.1

rmt-server-debuginfo-1.1.1-lp150.2.12.1

147628 - SuSE Linux 15.0 openSUSE-SU-2019:0167-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

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

openSUSE-SU-2019:0167-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00054.html>

SuSE Linux 15.0

x86_64

libspice-server1-debuginfo-0.14.0-lp150.3.6.1

spice-debugsource-0.14.0-lp150.3.6.1

libspice-server-devel-0.14.0-lp150.3.6.1

libspice-server1-0.14.0-lp150.3.6.1

i586

libspice-server1-debuginfo-0.14.0-lp150.3.6.1

spice-debugsource-0.14.0-lp150.3.6.1

libspice-server-devel-0.14.0-lp150.3.6.1

libspice-server1-0.14.0-lp150.3.6.1

147639 - SuSE Linux 42.3 openSUSE-SU-2019:0176-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

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

openSUSE-SU-2019:0176-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00069.html>

SuSE Linux 42.3

x86_64
spice-debugsource-0.12.8-13.1
libspice-server-devel-0.12.8-13.1
libspice-server1-0.12.8-13.1
libspice-server1-debuginfo-0.12.8-13.1

147646 - SuSE Linux 15.0 openSUSE-SU-2019:0215-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7397

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0215-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00106.html>

SuSE Linux 15.0

x86_64
libGraphicsMagickWand-Q16-2-debuginfo-1.3.29-lp150.3.21.1
GraphicsMagick-devel-1.3.29-lp150.3.21.1
perl-GraphicsMagick-debuginfo-1.3.29-lp150.3.21.1
libGraphicsMagick++-Q16-12-1.3.29-lp150.3.21.1
libGraphicsMagick3-config-1.3.29-lp150.3.21.1
libGraphicsMagickWand-Q16-2-1.3.29-lp150.3.21.1
perl-GraphicsMagick-1.3.29-lp150.3.21.1
libGraphicsMagick-Q16-3-1.3.29-lp150.3.21.1
libGraphicsMagick++-devel-1.3.29-lp150.3.21.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.29-lp150.3.21.1
GraphicsMagick-1.3.29-lp150.3.21.1
GraphicsMagick-debuginfo-1.3.29-lp150.3.21.1
GraphicsMagick-debugsource-1.3.29-lp150.3.21.1
libGraphicsMagick-Q16-3-debuginfo-1.3.29-lp150.3.21.1

147650 - SuSE Linux 15.0 openSUSE-SU-2019:0163-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1000021

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0163-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00051.html>

SuSE Linux 15.0

x86_64
python3-slixmpp-1.3.0-lp150.2.3.1
python-slixmpp-debugsource-1.3.0-lp150.2.3.1
python3-slixmpp-debuginfo-1.3.0-lp150.2.3.1

147651 - SuSE Linux 15.0 openSUSE-SU-2019:0203-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20669, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0203-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00094.html>

SuSE Linux 15.0

x86_64
kernel-vanilla-devel-debuginfo-4.12.14-lp150.12.48.1
kernel-debug-base-4.12.14-lp150.12.48.1
kernel-kvmsmall-devel-4.12.14-lp150.12.48.1
kernel-debug-4.12.14-lp150.12.48.1
kernel-default-base-debuginfo-4.12.14-lp150.12.48.1
kernel-obs-build-debugsource-4.12.14-lp150.12.48.1
kernel-kvmsmall-base-debuginfo-4.12.14-lp150.12.48.1
kernel-kvmsmall-debuginfo-4.12.14-lp150.12.48.1
kernel-default-devel-debuginfo-4.12.14-lp150.12.48.1
kernel-kvmsmall-base-4.12.14-lp150.12.48.1
kernel-default-debugsource-4.12.14-lp150.12.48.1
kernel-obs-build-4.12.14-lp150.12.48.1
kernel-syms-4.12.14-lp150.12.48.1
kernel-vanilla-base-debuginfo-4.12.14-lp150.12.48.1
kernel-default-debuginfo-4.12.14-lp150.12.48.1
kernel-vanilla-4.12.14-lp150.12.48.1
kernel-vanilla-debuginfo-4.12.14-lp150.12.48.1
kernel-default-base-4.12.14-lp150.12.48.1
kernel-debug-base-debuginfo-4.12.14-lp150.12.48.1
kernel-debug-debuginfo-4.12.14-lp150.12.48.1
kernel-debug-devel-debuginfo-4.12.14-lp150.12.48.1
kernel-vanilla-base-4.12.14-lp150.12.48.1
kernel-vanilla-debugsource-4.12.14-lp150.12.48.1
kernel-debug-debugsource-4.12.14-lp150.12.48.1
kernel-default-devel-4.12.14-lp150.12.48.1
kernel-debug-devel-4.12.14-lp150.12.48.1
kernel-obs-qa-4.12.14-lp150.12.48.1
kernel-vanilla-devel-4.12.14-lp150.12.48.1
kernel-kvmsmall-devel-debuginfo-4.12.14-lp150.12.48.1
kernel-kvmsmall-4.12.14-lp150.12.48.1
kernel-kvmsmall-debugsource-4.12.14-lp150.12.48.1
kernel-default-4.12.14-lp150.12.48.1

noarch

kernel-source-vanilla-4.12.14-lp150.12.48.1

kernel-devel-4.12.14-lp150.12.48.1
kernel-source-4.12.14-lp150.12.48.1
kernel-docs-4.12.14-lp150.12.48.1
kernel-docs-html-4.12.14-lp150.12.48.1
kernel-macros-4.12.14-lp150.12.48.1

147653 - SuSE Linux 42.3 openSUSE-SU-2019:0214-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7397

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0214-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00104.html>

SuSE Linux 42.3

x86_64

GraphicsMagick-debuginfo-1.3.25-126.1
libGraphicsMagickWand-Q16-2-1.3.25-126.1
libGraphicsMagick-Q16-3-1.3.25-126.1
GraphicsMagick-1.3.25-126.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-126.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-126.1
libGraphicsMagick++-Q16-12-1.3.25-126.1
libGraphicsMagick++-devel-1.3.25-126.1
perl-GraphicsMagick-1.3.25-126.1
perl-GraphicsMagick-debuginfo-1.3.25-126.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-126.1
GraphicsMagick-devel-1.3.25-126.1
GraphicsMagick-debugsource-1.3.25-126.1
libGraphicsMagick3-config-1.3.25-126.1

i586

GraphicsMagick-debuginfo-1.3.25-126.1
libGraphicsMagickWand-Q16-2-1.3.25-126.1
libGraphicsMagick-Q16-3-1.3.25-126.1
GraphicsMagick-1.3.25-126.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-126.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-126.1
libGraphicsMagick++-Q16-12-1.3.25-126.1
libGraphicsMagick++-devel-1.3.25-126.1
perl-GraphicsMagick-1.3.25-126.1
perl-GraphicsMagick-debuginfo-1.3.25-126.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-126.1
GraphicsMagick-devel-1.3.25-126.1
GraphicsMagick-debugsource-1.3.25-126.1
libGraphicsMagick3-config-1.3.25-126.1

182916 - FreeBSD msmtplib Certificate-verification Issue (f0416fb5-3130-11e9-a5ba-e0d55e883e26)

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

Risk Level: Medium
CVE: CVE-2019-8337

Description

The scan detected that the host is missing the following update:
msmtp -- certificate-verification issue (f0416fb5-3130-11e9-a5ba-e0d55e883e26)

Observation

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

<http://www.vuxml.org/freebsd/f0416fb5-3130-11e9-a5ba-e0d55e883e26.html>

Affected packages:
1.8.1 < msmtp < 1.8.3

186578 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3890-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2019-6975

Description

The scan detected that the host is missing the following update:
USN-3890-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004772.html>

Ubuntu 16.04

python-django_1.8.7-1ubuntu5.8
python3-django_1.8.7-1ubuntu5.8

Ubuntu 18.10

python-django_1.11.15-1ubuntu1.2
python3-django_1.11.15-1ubuntu1.2

Ubuntu 18.04

python-django_1.11.11-1ubuntu1.3
python3-django_1.11.11-1ubuntu1.3

194799 - Fedora Linux 28 FEDORA-2019-1f81367ac3 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2018-11803

Description

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

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/2019/2/?count=200&page=1>

Fedora Core 28

subversion-1.11.1-1.fc28

24743 - Joomla Stored XSS Issue In The Global Configuration Textfilter Settings Vulnerability (20190103)

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

Risk Level: Medium

CVE: CVE-2019-6263

Description

A stored xss vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A stored xss vulnerability is present in some versions of Joomla! CMS. The flaw lies in the Global Configuration text filter settings. Successful exploitation could allow a malicious user to bypass security and steal cookie-based authentication credentials.

24752 - (JSA10902) Juniper Junos OS Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0003

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in routing protocol daemon process. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

163810 - Oracle Enterprise Linux ELSA-2019-0375 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-8308

Description

The scan detected that the host is missing the following update:
ELSA-2019-0375

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-February/008490.html>

OEL7
x86_64
flatpak-builder-1.0.0-4.el7_6
flatpak-devel-1.0.2-4.el7_6
flatpak-libs-1.0.2-4.el7_6
flatpak-1.0.2-4.el7_6

194781 - Fedora Linux 29 FEDORA-2019-44a9d99647 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7146, CVE-2019-7148, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665

Description

The scan detected that the host is missing the following update:
FEDORA-2019-44a9d99647

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/2019/2/?count=200&page=1>

Fedora Core 29

elfutils-0.176-1.fc29

194788 - Fedora Linux 29 FEDORA-2019-095c760511 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5773

Description

The scan detected that the host is missing the following update:
FEDORA-2019-095c760511

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/2019/2/?count=200&page=1>

Fedora Core 29

python-markdown2-2.3.7-1.fc29

194792 - Fedora Linux 29 FEDORA-2019-b0bd3c604a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16646, CVE-2018-19058, CVE-2018-19059, CVE-2018-19060, CVE-2018-19149, CVE-2018-20481, CVE-2018-20551, CVE-2018-20650

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b0bd3c604a

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/2019/2/?count=200&page=1>

Fedora Core 29

mingw-poppler-0.67.0-3.fc29

194797 - Fedora Linux 28 FEDORA-2019-a16e1127d3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5773

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a16e1127d3

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/2019/2/?count=200&page=1>

Fedora Core 28

python-markdown2-2.3.7-1.fc28

196252 - Red Hat Enterprise Linux RHSA-2019-0375 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-8308

Description

The scan detected that the host is missing the following update:
RHSA-2019-0375

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-February/msg00024.html>

RHEL7D
x86_64
flatpak-builder-1.0.0-4.el7_6
flatpak-debuginfo-1.0.2-4.el7_6
flatpak-libs-1.0.2-4.el7_6
flatpak-devel-1.0.2-4.el7_6
flatpak-1.0.2-4.el7_6

RHEL7S
x86_64
flatpak-builder-1.0.0-4.el7_6
flatpak-debuginfo-1.0.2-4.el7_6
flatpak-libs-1.0.2-4.el7_6
flatpak-devel-1.0.2-4.el7_6
flatpak-1.0.2-4.el7_6

RHEL7WS
x86_64
flatpak-builder-1.0.0-4.el7_6
flatpak-debuginfo-1.0.2-4.el7_6
flatpak-libs-1.0.2-4.el7_6
flatpak-devel-1.0.2-4.el7_6
flatpak-1.0.2-4.el7_6

131299 - Debian Linux 9.0 DSA-4393-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
DSA-4393-1

Observation

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

<http://www.debian.org/security/2019/dsa-4393>

Debian 9.0
all
systemd_232-25+deb9u9

131300 - Debian Linux 9.0 DSA-4390-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-4390-1

Observation

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

<http://www.debian.org/security/2019/dsa-4390>

Debian 9.0
all
flatpak_0.8.9-0+deb9u2

147633 - SuSE Linux 42.3 openSUSE-SU-2019:0199-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20340

Description

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

openSUSE-SU-2019:0199-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-02/msg00087.html>

SuSE Linux 42.3
x86_64
libu2f-host0-1.0.0-5.3.1
libu2f-host-debugsource-1.0.0-5.3.1
libu2f-host-doc-1.0.0-5.3.1
u2f-host-1.0.0-5.3.1
libu2f-host-devel-1.0.0-5.3.1
libu2f-host0-debuginfo-1.0.0-5.3.1
u2f-host-debuginfo-1.0.0-5.3.1

147658 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0435-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-16872, CVE-2018-18954, CVE-2018-19364, CVE-2018-19489, CVE-2019-6778

Description

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

SUSE-SU-2019:0435-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005136.html>

SuSE SLED 12 SP4
x86_64
qemu-debugsource-2.11.2-5.8.1
qemu-x86-2.11.2-5.8.1
qemu-block-curl-2.11.2-5.8.1

qemu-tools-debuginfo-2.11.2-5.8.1
qemu-kvm-2.11.2-5.8.1
qemu-tools-2.11.2-5.8.1
qemu-2.11.2-5.8.1
qemu-block-curl-debuginfo-2.11.2-5.8.1

noarch
qemu-ipxe-1.0.0+-5.8.1
qemu-vgabios-1.11.0-5.8.1
qemu-seabios-1.11.0-5.8.1
qemu-sgabios-8-5.8.1

SuSE SLES 12 SP4
noarch
qemu-ipxe-1.0.0+-5.8.1
qemu-vgabios-1.11.0-5.8.1
qemu-seabios-1.11.0-5.8.1
qemu-sgabios-8-5.8.1

x86_64
qemu-block-curl-2.11.2-5.8.1
qemu-block-ssh-debuginfo-2.11.2-5.8.1
qemu-block-rbd-debuginfo-2.11.2-5.8.1
qemu-block-iscsi-2.11.2-5.8.1
qemu-guest-agent-2.11.2-5.8.1
qemu-block-curl-debuginfo-2.11.2-5.8.1
qemu-2.11.2-5.8.1
qemu-tools-2.11.2-5.8.1
qemu-block-iscsi-debuginfo-2.11.2-5.8.1
qemu-guest-agent-debuginfo-2.11.2-5.8.1
qemu-x86-2.11.2-5.8.1
qemu-tools-debuginfo-2.11.2-5.8.1
qemu-block-rbd-2.11.2-5.8.1
qemu-lang-2.11.2-5.8.1
qemu-debugsource-2.11.2-5.8.1
qemu-kvm-2.11.2-5.8.1
qemu-block-ssh-2.11.2-5.8.1

186577 - Ubuntu Linux 18.04, 18.10 USN-3889-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6212, CVE-2019-6215

Description

The scan detected that the host is missing the following update:
USN-3889-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004771.html>

Ubuntu 18.10

libjavascriptcoregtk-4.0-18_2.22.6-0ubuntu0.18.10.1
libwebkit2gtk-4.0-37_2.22.6-0ubuntu0.18.10.1

Ubuntu 18.04

libwebkit2gtk-4.0-37_2.22.6-0ubuntu0.18.04.1

libjavascriptcoregtk-4.0-18_2.22.6-0ubuntu0.18.04.1

186579 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3891-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
USN-3891-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004774.html>

Ubuntu 16.04

systemd_229-4ubuntu21.16

libsystemd0_229-4ubuntu21.16

Ubuntu 18.10

systemd_239-7ubuntu10.8

libsystemd0_239-7ubuntu10.8

Ubuntu 18.04

libsystemd0_237-3ubuntu10.13

systemd_237-3ubuntu10.13

194775 - Fedora Linux 28 FEDORA-2019-8cbe2a05cd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12546, CVE-2018-12550, CVE-2018-12551

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8cbe2a05cd

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/2019/2/?count=200&page=1>

Fedora Core 28

mosquitto-1.5.6-1.fc28

194777 - Fedora Linux 28 FEDORA-2019-75ee9101ea 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-2019-75ee9101ea

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/2019/2/?count=200&page=1>

Fedora Core 28

netmask-2.4.4-1.fc28

194778 - Fedora Linux 29 FEDORA-2019-68b9bec5ca Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-18508

Description

The scan detected that the host is missing the following update:
FEDORA-2019-68b9bec5ca

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/2019/2/?count=200&page=2>

Fedora Core 29

nss-3.42.1-1.fc29

194780 - Fedora Linux 28 FEDORA-2019-ef5551fcff Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-18898

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ef5551fcff

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/2019/2/?count=200&page=2>

Fedora Core 28

perl-Email-Address-List-0.06-1.fc28

194782 - Fedora Linux 28 FEDORA-2019-8e683d3810 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7443

Description

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

FEDORA-2019-8e683d3810

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/2019/2/?count=200&page=1>

Fedora Core 28

kf5-kauth-5.54.0-2.fc28

194783 - Fedora Linux 29 FEDORA-2019-19b1d53695 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7443

Description

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

FEDORA-2019-19b1d53695

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/2019/2/?count=200&page=1>

Fedora Core 29

kf5-kauth-5.54.0-2.fc29

194786 - Fedora Linux 29 FEDORA-2019-af3d726d38 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7639

Description

The scan detected that the host is missing the following update:
FEDORA-2019-af3d726d38

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/2019/2/?count=200&page=1>

Fedora Core 29

gsi-openssh-7.9p1-5.fc29

194798 - Fedora Linux 29 FEDORA-2019-d645f4337d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6212, CVE-2019-6215

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d645f4337d

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/2019/2/?count=200&page=2>

Fedora Core 29

webkit2gtk3-2.22.6-1.fc29

194800 - Fedora Linux 28 FEDORA-2019-710afd062a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7639

Description

The scan detected that the host is missing the following update:
FEDORA-2019-710afd062a

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/2019/2/?count=200&page=1>

Fedora Core 28

gsi-openssh-7.8p1-3.fc28

194802 - Fedora Linux 29 FEDORA-2019-0723b8f333 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-2019-0723b8f333

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/2019/2/?count=200&page=1>

Fedora Core 29

netmask-2.4.4-1.fc29

147647 - SuSE SLES 11 SP4 SUSE-SU-2019:13962-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-19364, CVE-2018-19489, CVE-2019-6778

Description

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

SUSE-SU-2019:13962-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-February/005126.html>

SuSE SLES 11 SP4

i586

kvm-1.4.2-60.21.1

x86_64

kvm-1.4.2-60.21.1

ENHANCED CHECKS

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

11763 - (MS11-027) Cumulative Security Update of ActiveX Kill Bits (2508272)

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

Risk Level: High

CVE: CVE-2010-0811, CVE-2010-3973, CVE-2011-1243

Update Details

FASLScript is updated

13073 - (MS11-090) Cumulative Security Update of ActiveX Kill Bits (2618451)

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

Risk Level: High

CVE: CVE-2011-3397

Update Details

FASLScript is updated

131276 - Debian Linux 9.0 DSA-4371-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3462

Update Details

Risk is updated

171069 - Amazon Linux AMI ALAS-2019-1156 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Update Details

Risk is updated

186541 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3863-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3462

Update Details

Risk is updated

194751 - Fedora Linux 29 FEDORA-2019-fd9345f44a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Update Details

Risk is updated

131277 - Debian Linux 9.0 DSA-4370-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6338, CVE-2019-6339

[Update Details](#)

Risk is updated

131279 - Debian Linux 9.0 DSA-4373-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-4056, CVE-2018-4058, CVE-2018-4059

[Update Details](#)

Risk is updated

182904 - FreeBSD turnserver Multiple Vulnerabilities (181beef6-2482-11e9-b4a3-00155d006b02)

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

Risk Level: High

CVE: CVE-2018-4056, CVE-2018-4058, CVE-2018-4059

[Update Details](#)

Risk is updated

194757 - Fedora Linux 29 FEDORA-2019-e66b1889ec Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6438

[Update Details](#)

Risk is updated CVE is updated

24659 - (HT209443) Apple iOS Multiple Vulnerabilities Prior To 12.1.3

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2019-6200, CVE-2019-6202, CVE-2019-6205, CVE-2019-6206, CVE-2019-6208, CVE-2019-6209, CVE-2019-6210, CVE-2019-6211, CVE-2019-6212, CVE-2019-6213, CVE-2019-6214, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6218, CVE-2019-6219, CVE-2019-6221, CVE-2019-6224, CVE-2019-6225, CVE-2019-6226, CVE-2019-6227, CVE-2019-6228, CVE-2019-6229, CVE-2019-6230, CVE-2019-6231, CVE-2019-6233, CVE-2019-6234, CVE-2019-6235

[Update Details](#)

Risk is updated

24660 - (HT209446) Apple macOS Multiple Vulnerabilities Prior To 10.14.3

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2018-4452, CVE-2018-4467, CVE-2019-6200, CVE-2019-6202, CVE-2019-6205, CVE-2019-6208, CVE-2019-6209, CVE-2019-6210, CVE-2019-6211, CVE-2019-6213, CVE-2019-6214, CVE-2019-6218, CVE-2019-6219, CVE-2019-6220, CVE-2019-6221, CVE-2019-6224, CVE-2019-6225, CVE-2019-6230, CVE-2019-

6231, CVE-2019-6235

[Update Details](#)

Risk is updated

24670 - (HT209451) Apple iCloud Vulnerabilities Prior To 7.10

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

Risk Level: Medium

CVE: CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

[Update Details](#)

Risk is updated

147548 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0054-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20683

[Update Details](#)

Risk is updated

182873 - FreeBSD couchdb Administrator Privilege Escalation (1999a215-fc6b-11e8-8a95-ac1f6b67e138)

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

Risk Level: Medium

CVE: CVE-2018-17188

[Update Details](#)

Risk is updated

196249 - Red Hat Enterprise Linux RHSA-2019-0309 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782

[Update Details](#)

Risk is updated

24667 - Apache HTTP Server Multiple Vulnerabilities Prior To 2.4.38

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0190

[Update Details](#)

Risk is updated

24674 - (MSPT-Feb2019) Microsoft Win32k Kernel Information Disclosure (CVE-2019-0628)

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

Risk Level: Medium

CVE: CVE-2019-0628

[Update Details](#)

Name is updated

88957 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-192-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5738

[Update Details](#)

Risk is updated

88997 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-022-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0190

[Update Details](#)

Risk is updated

182894 - FreeBSD Apache Vulnerability (eb888ce5-1f19-11e9-be05-4c72b94353b5)

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0190

[Update Details](#)

Risk is updated

186265 - Ubuntu Linux 18.04 USN-3683-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5738

[Update Details](#)

Risk is updated

193894 - Fedora Linux 28 FEDORA-2018-bfec61fb2f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5738

[Update Details](#)

Risk is updated

131269 - Debian Linux 9.0 DSA-4363-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3498

[Update Details](#)

Risk is updated

131271 - Debian Linux 9.0 DSA-4365-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3461

[Update Details](#)

Risk is updated

182883 - FreeBSD Django Content Spoofing Possibility In The Default 404 Page (3e41c1a6-10bc-11e9-bd85-fcaa147e860e)

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

Risk Level: Medium

CVE: CVE-2019-3498

[Update Details](#)

Risk is updated

186535 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3851-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3498

[Update Details](#)

Risk is updated

194670 - Fedora Linux 29 FEDORA-2019-a7b53ed5a3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3498

[Update Details](#)

Risk is updated

194701 - Fedora Linux 28 FEDORA-2019-e6ca5847c7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3498

[Update Details](#)

Risk is updated

147505 - SuSE Linux 15.0 openSUSE-SU-2018:4272-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-17957

[Update Details](#)

Risk is updated

147564 - SuSE Linux 15.0 openSUSE-SU-2019:0057-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20483

[Update Details](#)

Risk is updated

186525 - Ubuntu Linux 18.04 USN-3856-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10910

[Update Details](#)

Risk is updated

194650 - Fedora Linux 29 FEDORA-2019-088875c43a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20483

[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

70086 - oracle.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

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

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

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2019 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates