NEW CHECKS

25759 - Google Chrome Multiple Vulnerabilities Prior To 77.0.3865.120
Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High

Description
Multiple vulnerabilities are present in some versions of Google Chrome.

Observation
Google Chrome is a popular web browser.
Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to affect integrity, confidentiality and availability of the target.

25839 - Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Default SSH Key Vulnerability (cisco-sa-20190501)
Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2019-1804

Description
A vulnerability is present in some versions of Cisco NX-OS Software.

Observation
Cisco NX-OS Software is the operating system used in Cisco Nexus devices.
A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in SSH key management. Successful exploitation could allow an attacker to gain root user privileges on the target system.

25841 - (APSB19-44) Vulnerabilities In Adobe Photoshop CC
Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
Multiple vulnerabilities are present in some versions of Adobe Photoshop CC.

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

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

**25751 - Cisco Adaptive Security Appliance Software FTP Inspection Denial Of Service Vulnerability (cisco-sa-20191002-asa-dos)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2019-12673

Description
A vulnerability is present in some versions of Cisco ASA Software.

Observation
Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco ASA Software. The flaw lies in FTP inspection engine feature of Cisco Adaptive Security Appliance (ASA) Software. Successful exploitation could allow an unauthenticated remote attacker to cause a denial of service condition on the target system.


Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-12669

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 is in the RADIUS Change of Authorization (CoA) code of Cisco IOS XE Software. Successful exploitation could allow an attacker to cause a denial of service condition in the target system.

**25764 - WordPress Multiple Vulnerabilities Prior To 5.2.4**

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: High
CVE: CVE-MAP-NOMATCH

Description
Multiple vulnerabilities are present in some versions of WordPress.

Observation
WordPress is a popular blog application.
Multiple vulnerabilities are present in some versions of WordPress. The flaws lie in multiple components. Successful exploitation could allow an attacker to perform cross-site scripting attacks.

131477 - Debian Linux 10.0 DSA-4572-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-12838

Description
The scan detected that the host is missing the following update:
DSA-4572-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2019/dsa-4572

Debian 10.0
all
libpmi0-dev_18.08.5.2-1+deb10u1
slurmd_db_18.08.5.2-1+deb10u1
libpmi2-0-dev_18.08.5.2-1+deb10u1
libpmi0_18.08.5.2-1+deb10u1
slurm-wlm_18.08.5.2-1+deb10u1
libpam-slurm_18.08.5.2-1+deb10u1
slurmctl_18.08.5.2-1+deb10u1
sview_18.08.5.2-1+deb10u1
slurmd_18.08.5.2-1+deb10u1
libslurm-dev_18.08.5.2-1+deb10u1
slurm-client_18.08.5.2-1+deb10u1
libslurm33_18.08.5.2-1+deb10u1
slurm-client-emulator_18.08.5.2-1+deb10u1
libslurmdb-perl_18.08.5.2-1+deb10u1
slurm-wlm-torque_18.08.5.2-1+deb10u1
libslurmdb33_18.08.5.2-1+deb10u1
slurm-wlm-basic-plugins-dev_18.08.5.2-1+deb10u1

132522 - Oracle VM OVMSA-2019-0054 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-12207

Description
The scan detected that the host is missing the following update:
OVMSA-2019-0054
Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:


OVM3.4
x86_64
xen-4.4.4-155.0.75.el6
xen-tools-4.4.4-155.0.75.el6

148534 - SuSE Linux 15.0 openSUSE-SU-2019:2530-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-2201

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2530-1

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


SuSE Linux 15.0
x86_64
libjpeg-turbo-1.5.3-lp150.4.7.1
libjpeg62-62.2.0-lp150.4.7.1
libjpeg62-turbo-1.5.3-lp150.4.7.1
libjpeg62-turbo-1.5.3-lp150.4.7.1
libjpeg62-turbo-1.5.3-lp150.4.7.1
libjpeg62-debugsource-1.5.3-lp150.4.7.1
libjpeg62-debuginfo-62.2.0-lp150.4.7.1
libjpeg-turbo-debugsource-1.5.3-lp150.4.7.1
libjpeg8-32bit-debuginfo-8.1.2-lp150.4.7.1
libjpeg8-devel-32bit-8.1.2-lp150.4.7.1
libjpeg8-debuginfo-8.1.2-lp150.4.7.1
libjpeg8-devel-8.1.2-lp150.4.7.1
libturbojpeg0-8.1.2-lp150.4.7.1
libturbojpeg0-32bit-debuginfo-8.1.2-lp150.4.7.1
libjpeg62-32bit-62.2.0-lp150.4.7.1
libjpeg62-devel-32bit-62.2.0-lp150.4.7.1
libturbojpeg0-debuginfo-8.1.2-lp150.4.7.1
libjpeg62-devel-32bit-62.2.0-lp150.4.7.1
libjpeg-turbo-debuginfo-1.5.3-lp150.4.7.1
libjpeg8-8.1.2-lp150.4.7.1
libjpeg62-32bit-debuginfo-62.2.0-lp150.4.7.1
libjpeg8-32bit-8.1.2-lp150.4.7.1
libjpeg62-32bit-debuginfo-62.2.0-lp150.4.7.1
libjpeg8-32bit-8.1.2-lp150.4.7.1
i586
libjpeg-turbo-1.5.3-lp150.4.7.1
libjpeg62-62.2.0-lp150.4.7.1
libjpeg62-turbo-1.5.3-lp150.4.7.1
libjpeg62-turbo-1.5.3-lp150.4.7.1
libjpeg62-turbo-1.5.3-lp150.4.7.1
libjpeg62-debugsource-1.5.3-lp150.4.7.1
libjpeg62-debuginfo-62.2.0-lp150.4.7.1
libjpeg8-turbo-debugsource-1.5.3-lp150.4.7.1
148535 - SuSE Linux 15.0 openSUSE-SU-2019:2506-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2506-1

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

SuSE Linux 15.0
x86_64
xen-debugsource-4.10.4_06-lp150.2.25.1
xen-doc-html-4.10.4_06-lp150.2.25.1
xen-libs-4.10.4_06-lp150.2.25.1
xen-tools-domU-4.10.4_06-lp150.2.25.1
xen-4.10.4_06-lp150.2.25.1
xen-libs-32bit-debuginfo-4.10.4_06-lp150.2.25.1
xen-libs-32bit-4.10.4_06-lp150.2.25.1
xen-devel-4.10.4_06-lp150.2.25.1
xen-tools-4.10.4_06-lp150.2.25.1
xen-libs-debuginfo-4.10.4_06-lp150.2.25.1
xen-tools-debuginfo-4.10.4_06-lp150.2.25.1
xen-tools-domU-debuginfo-4.10.4_06-lp150.2.25.1

i586
xen-debugsource-4.10.4_06-lp150.2.25.1
xen-libs-4.10.4_06-lp150.2.25.1
xen-tools-domU-4.10.4_06-lp150.2.25.1
xen-devel-4.10.4_06-lp150.2.25.1
xen-libs-debuginfo-4.10.4_06-lp150.2.25.1
xen-tools-domU-debuginfo-4.10.4_06-lp150.2.25.1

148536 - SuSE SLED 12 SP5 SUSE-SU-2019:2744-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-16239

Description
The scan detected that the host is missing the following update:
SUSE-SU-2019:2744-2
Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:


SuSE SLED 12 SP5
x86_64
openconnect-debuginfo-7.08-3.4.1
openconnect-7.08-3.4.1
openconnect-debugsource-7.08-3.4.1

noarch
openconnect-lang-7.08-3.4.1

148538 - SuSE Linux 15.1 openSUSE-SU-2019:2507-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2507-1

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


SuSE Linux 15.1
x86_64
kernel-default-debuginfo-4.12.14-lp151.28.32.1
kernel-kvmsmall-debugsource-4.12.14-lp151.28.32.1
kernel-vanilla-4.12.14-lp151.28.32.1
kernel-default-devel-4.12.14-lp151.28.32.1
kernel-default-base-debuginfo-4.12.14-lp151.28.32.1
kernel-kvmsmall-devel-debuginfo-4.12.14-lp151.28.32.1
kernel-vanilla-devel-4.12.14-lp151.28.32.1
kernel-debug-4.12.14-lp151.28.32.1
kernel-debug-devel-debuginfo-4.12.14-lp151.28.32.1
kernel-obs-qa-4.12.14-lp151.28.32.1
kernel-kvmsmall-base-4.12.14-lp151.28.32.1
kernel-default-devel-debuginfo-4.12.14-lp151.28.32.1
kernel-vanilla-base-4.12.14-lp151.28.32.1
kernel-syms-4.12.14-lp151.28.32.1
kernel-vanilla-devel-debuginfo-4.12.14-lp151.28.32.1
kernel-kvmsmall-debuginfo-4.12.14-lp151.28.32.1
kernel-default-build-debugsource-4.12.14-lp151.28.32.1
kernel-debug-debugsource-4.12.14-lp151.28.32.1
kernel-debug-debuginfo-4.12.14-lp151.28.32.1
kernel-vanilla-base-debuginfo-4.12.14-lp151.28.32.1
kernel-default-base-4.12.14-lp151.28.32.1
148539 - SuSE SLES 12 SP5, SLED 12 SP5 SUSE-SU-2019:2785-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
SUSE-SU-2019:2785-2

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

SuSE SLED 12 SP5
x86_64
ImageMagick-debuginfo-6.8.8.1-71.131.1
ImageMagick-6.8.8.1-71.131.1
ImageMagick-debugsource-6.8.8.1-71.131.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.131.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.131.1
libMagick++-6_Q16-3-6.8.8.1-71.131.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.131.1

SuSE SLES 12 SP5
x86_64
ImageMagick-debuginfo-6.8.8.1-71.131.1
ImageMagick-config-6-upstream-6.8.8.1-71.131.1
ImageMagick-config-6-SUSE-6.8.8.1-71.131.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.131.1
libMagickWand-6_Q16-1-6.8.8.1-71.131.1
ImageMagick-debugsource-6.8.8.1-71.131.1
libMagickCore-6_Q16-1-6.8.8.1-71.131.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.131.1

148540 - SuSE Linux 15.0 openSUSE-SU-2019:2527-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2527-1

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

SuSE Linux 15.0
x86_64
ucode-intel-20191112a-lp150.2.33.1

148541 - SuSE Linux 15.1 openSUSE-SU-2019:2514-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-17362

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2514-1

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

SuSE Linux 15.1
x86_64
libtomcrypt-debugsource-1.17-lp151.3.3.1
libtomcrypt0-debuginfo-1.17-lp151.3.3.1
libtomcrypt-examples-1.17-lp151.3.3.1
libtomcrypt-1.17-lp151.3.3.1
libtomcrypt-devel-1.17-lp151.3.3.1

148542 - SuSE Linux 15.1 openSUSE-SU-2019:2529-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-2201

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2529-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
SuSE Linux 15.1

x86_64
libjpeg8-devel-32bit-8.1.2-lp151.6.3.1
libturbojpeg0-32bit-debuginfo-8.1.2-lp151.6.3.1
libjpeg8-32bit-debuginfo-8.1.2-lp151.6.3.1
libjpeg62-32bit-debuginfo-62.2.0-lp151.6.3.1
libjpeg62-debuginfo-62.2.0-lp151.6.3.1
libjpeg8-32bit-8.1.2-lp151.6.3.1
libjpeg-turbo-debuginfo-1.5.3-lp151.6.3.1
libjpeg62-62.2.0-lp151.6.3.1
libjpeg62-devel-62.2.0-lp151.6.3.1
libjpeg-turbo-1.5.3-lp151.6.3.1
libturbojpeg0-debuginfo-8.1.2-lp151.6.3.1
libjpeg-turbo-debugsource-1.5.3-lp151.6.3.1
libjpeg8-devel-8.1.2-lp151.6.3.1
libturbojpeg0-8.1.2-lp151.6.3.1
libjpeg8-debuginfo-8.1.2-lp151.6.3.1
libjpeg62-turbo-debugsource-1.5.3-lp151.6.3.1
libjpeg62-32bit-62.2.0-lp151.6.3.1
libjpeg8-8.1.2-lp151.6.3.1
libjpeg62-devel-32bit-62.2.0-lp151.6.3.1
libturbojpeg0-8.1.2-lp151.6.3.1
libjpeg62-turbo-1.5.3-lp151.6.3.1

i586
libjpeg62-debuginfo-62.2.0-lp151.6.3.1
libjpeg-turbo-debuginfo-1.5.3-lp151.6.3.1
libjpeg62-62.2.0-lp151.6.3.1
libjpeg62-devel-62.2.0-lp151.6.3.1
libjpeg-turbo-1.5.3-lp151.6.3.1
libturbojpeg0-debuginfo-8.1.2-lp151.6.3.1
libjpeg-turbo-debugsource-1.5.3-lp151.6.3.1
libjpeg8-devel-8.1.2-lp151.6.3.1
libjpeg8-debuginfo-8.1.2-lp151.6.3.1
libjpeg62-turbo-debugsource-1.5.3-lp151.6.3.1
libjpeg8-8.1.2-lp151.6.3.1
libturbojpeg0-8.1.2-lp151.6.3.1
libjpeg62-turbo-1.5.3-lp151.6.3.1

148543 - SuSE Linux 15.0 openSUSE-SU-2019:2521-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2521-1

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

148544 - SuSE Linux 15.1 openSUSE-SU-2019:2522-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2522-1

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

148545 - SuSE Linux 15.1 openSUSE-SU-2019:2509-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2509-1

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

148546 - SuSE Linux 15.1 openSUSE-SU-2019:2515-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
**Description**

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

openSUSE-SU-2019:2515-1

**Observation**

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


SuSE Linux 15.1

i586

libMagick++-devel-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-7.0.7.34-lp151.7.12.1
perl-PerlMagick-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-debuginfo-7.0.7.34-lp151.7.12.1
perl-PerlMagick-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-config-7-SUSE-7.0.7.34-lp151.7.12.1
ImageMagick-extra-7.0.7.34-lp151.7.12.1
ImageMagick-debugsource-7.0.7.34-lp151.7.12.1
ImageMagick-debuginfo-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-debuginfo-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-7.0.7.34-lp151.7.12.1
ImageMagick-extra-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-config-7-upstream-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-debuginfo-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-32bit-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-32bit-debuginfo-7.0.7.34-lp151.7.12.1
libMagick++-devel-32bit-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-7.0.7.34-lp151.7.12.1
ImageMagick-devel-32bit-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-devel-32bit-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-32bit-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-debuginfo-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-debuginfo-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-config-7-upstream-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-32bit-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-32bit-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-32bit-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagick++-7_Q16HDR|4-32bit-debuginfo-7.0.7.34-lp151.7.12.1
ImageMagick-devel-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
libMagickCore-7_Q16HDR|6-32bit-7.0.7.34-lp151.7.12.1
libMagickWand-7_Q16HDR|6-7.0.7.34-lp151.7.12.1
148547 - SuSE SLED 15, 15 SP1 SUSE-SU-2019:2982-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-MAP-NOMATCH

Description
The scan detected that the host is missing the following update:
SUSE-SU-2019:2982-1

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

SuSE SLED 15
x86_64
enigmail-2.1.2-3.19.1

SuSE SLED 15 SP1
x86_64
enigmail-2.1.2-3.19.1

148548 - SuSE Linux 15.0 openSUSE-SU-2019:2519-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2519-1

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

SuSE Linux 15.0
i586
perl-PerlMagick-7.0.7.34-lp150.2.41.1
ImageMagick-debugsource-7.0.7.34-lp150.2.41.1
ImageMagick-extra-7.0.7.34-lp150.2.41.1
libMagick++-7_Q16HDR16-7.0.7.34-lp150.2.41.1
ImageMagick-config-7-upstream-7.0.7.34-lp150.2.41.1
libMagickWand-7_Q16HDR16-7.0.7.34-lp150.2.41.1
libMagickWand-7_Q16HDR16-debuginfo-7.0.7.34-lp150.2.41.1
libMagickCore-7_Q16HDR16-debuginfo-7.0.7.34-lp150.2.41.1
ImageMagick-devel-7.0.7.34-lp150.2.41.1
ImageMagick-config-7-SUSE-7.0.7.34-lp150.2.41.1
libMagickCore-7_Q16HDR16-7.0.7.34-lp150.2.41.1
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-14869

Description
The scan detected that the host is missing the following update:
SUSE-SU-2019:2983-1

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

SuSE SLES 12 SP4
x86_64
ghostscript-debugsource-9.27-23.31.1
ghostscript-9.27-23.31.1
ghostscript-x11-9.27-23.31.1
SuSE SLED 12 SP4
x86_64
ghostscript-debugsource-9.27-23.31.1
ghostscript-9.27-23.31.1
ghostscript-x11-9.27-23.31.1
ghostscript-debuginfo-9.27-23.31.1
ghostscript-x11-debuginfo-9.27-23.31.1

SuSE SLES 12 SP5
x86_64
ghostscript-debugsource-9.27-23.31.1
ghostscript-9.27-23.31.1
ghostscript-x11-9.27-23.31.1
ghostscript-debuginfo-9.27-23.31.1
ghostscript-x11-debuginfo-9.27-23.31.1

148550 - SuSE Linux 15.1 openSUSE-SU-2019:2528-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2528-1

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

SuSE Linux 15.1
x86_64
ucode-intel-20191112a-lp151.2.12.1

148551 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:2988-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
SUSE-SU-2019:2988-1

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

SuSE SLED 12 SP4
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-2201

Description
The scan detected that the host is missing the following update:
SUSE-SU-2019:2972-1

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

SuSE SLES 12 SP4
x86_64
libjpeg8-8.1.2-31.19.1
libjpeg62-62.2.0-31.19.1
libjpeg62-debuginfo-32bit-62.2.0-31.19.1
libjpeg62-turbo-debugsource-1.5.3-31.19.1
libjpeg62-turbo-1.5.3-31.19.1
libturbojpeg0-8.1.2-31.19.1
libjpeg-turbo-debugsource-1.5.3-31.19.1
libjpeg8-debuginfo-32bit-8.1.2-31.19.1
libjpeg62-debuginfo-62.2.0-31.19.1
libturbojpeg0-debuginfo-8.1.2-31.19.1
libjpeg-turbo-debuginfo-1.5.3-31.19.1
libjpeg8-debuginfo-8.1.2-31.19.1
libjpeg-turbo-1.5.3-31.19.1
libjpeg62-32bit-62.2.0-31.19.1
libjpeg8-32bit-8.1.2-31.19.1

SuSE SLED 12 SP4
x86_64
libjpeg8-8.1.2-31.19.1
libjpeg62-62.2.0-31.19.1
libturbojpeg0-8.1.2-31.19.1
libjpeg62-turbo-debugsource-1.5.3-31.19.1
libjpeg62-turbo-1.5.3-31.19.1
libjpeg-turbo-1.5.3-31.19.1
libjpeg8-debuginfo-32bit-8.1.2-31.19.1
libjpeg62-debuginfo-62.2.0-31.19.1
libturbojpeg0-debuginfo-8.1.2-31.19.1
libjpeg-turbo-debuginfo-1.5.3-31.19.1
libjpeg8-debuginfo-32bit-8.1.2-31.19.1
libjpeg62-debuginfo-32bit-62.2.0-31.19.1
160641 - CentOS 7 CESA-2019-3872 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0155

Description
The scan detected that the host is missing the following update:
CESA-2019-3872

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

CentOS 7
x86_64
kernel-tools-3.10.0-1062.4.3.el7
kernel-headers-3.10.0-1062.4.3.el7
kernel-debug-devel-3.10.0-1062.4.3.el7
kernel-tools-libs-3.10.0-1062.4.3.el7
bpftool-3.10.0-1062.4.3.el7
kernel-devel-3.10.0-1062.4.3.el7
kernel-3.10.0-1062.4.3.el7
python-perf-3.10.0-1062.4.3.el7
kernel-debug-3.10.0-1062.4.3.el7
perf-3.10.0-1062.4.3.el7
kernel-tools-libs-devel-3.10.0-1062.4.3.el7

noarch
kernel-abi-whitelists-3.10.0-1062.4.3.el7
kernel-doc-3.10.0-1062.4.3.el7
160642 - CentOS 6 CESA-2019-3878 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0155

Description
The scan detected that the host is missing the following update:
CESA-2019-3878

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

CentOS 6
i686
kernel-2.6.32-754.24.3.el6
kernel-headers-2.6.32-754.24.3.el6
kernel-devel-2.6.32-754.24.3.el6
perf-2.6.32-754.24.3.el6
python-perf-2.6.32-754.24.3.el6
kernel-debug-2.6.32-754.24.3.el6
kernel-debug-devel-2.6.32-754.24.3.el6

noarch
kernel-firmware-2.6.32-754.24.3.el6
kernel-abi-whitelists-2.6.32-754.24.3.el6
kernel-doc-2.6.32-754.24.3.el6

x86_64
kernel-2.6.32-754.24.3.el6
kernel-headers-2.6.32-754.24.3.el6
kernel-devel-2.6.32-754.24.3.el6
perf-2.6.32-754.24.3.el6
python-perf-2.6.32-754.24.3.el6
kernel-debug-2.6.32-754.24.3.el6
kernel-debug-devel-2.6.32-754.24.3.el6

160643 - CentOS 7 CESA-2019-3834 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
CESA-2019-3834

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
CentOS 7
x86_64
bpftool-3.10.0-1062.4.2.el7
kernel-tools-3.10.0-1062.4.2.el7
kernel-tools-libs-3.10.0-1062.4.2.el7
python-perf-3.10.0-1062.4.2.el7
kernel-tools-libs-devel-3.10.0-1062.4.2.el7
perf-3.10.0-1062.4.2.el7
kernel-headers-3.10.0-1062.4.2.el7
kernel-debug-devel-3.10.0-1062.4.2.el7
kernel-3.10.0-1062.4.2.el7
kernel-debug-3.10.0-1062.4.2.el7
kernel-devel-3.10.0-1062.4.2.el7
noarch
kernel-doc-3.10.0-1062.4.2.el7
kernel-abi-whitelists-3.10.0-1062.4.2.el7

164047 - Oracle Enterprise Linux ELSA-2019-3888 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
ELSA-2019-3888

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

OEL7
x86_64
ghostscript-cups-9.25-2.el7_7.3
libgs-devel-9.25-2.el7_7.3
ghostscript-9.25-2.el7_7.3
libgs-9.25-2.el7_7.3
ghostscript-doc-9.25-2.el7_7.3
ghostscript-gtk-9.25-2.el7_7.3

164048 - Oracle Enterprise Linux ELSA-2019-3878 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0155

Description
The scan detected that the host is missing the following update:
ELSA-2019-3878

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


OEL6
x86_64
kernel-2.6.32-754.24.3.el6
kernel-doc-2.6.32-754.24.3.el6
kernel-firmware-2.6.32-754.24.3.el6
kernel-headers-2.6.32-754.24.3.el6
kernel-devel-2.6.32-754.24.3.el6
perf-2.6.32-754.24.3.el6
kernel-abi-whitelists-2.6.32-754.24.3.el6
python-perf-2.6.32-754.24.3.el6
kernel-debug-2.6.32-754.24.3.el6
kernel-debug-devel-2.6.32-754.24.3.el6

i386
kernel-2.6.32-754.24.3.el6
kernel-doc-2.6.32-754.24.3.el6
kernel-firmware-2.6.32-754.24.3.el6
kernel-headers-2.6.32-754.24.3.el6
kernel-devel-2.6.32-754.24.3.el6
perf-2.6.32-754.24.3.el6
kernel-abi-whitelists-2.6.32-754.24.3.el6
python-perf-2.6.32-754.24.3.el6
kernel-debug-2.6.32-754.24.3.el6
kernel-debug-devel-2.6.32-754.24.3.el6

164049 - Oracle Enterprise Linux ELSA-2019-3872 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ELSA-2019-3872

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


OEL7
x86_64
kernel-debug-devel-3.10.0-1062.4.3.el7
kernel-3.10.0-1062.4.3.el7
perf-3.10.0-1062.4.3.el7
python-perf-3.10.0-1062.4.3.el7
kernel-tools-3.10.0-1062.4.3.el7
kernel-doc-3.10.0-1062.4.3.el7
kernel-debug-3.10.0-1062.4.3.el7
kernel-devel-3.10.0-1062.4.3.el7
bpftool-3.10.0-1062.4.3.el7
kernel-tools-libs-devel-3.10.0-1062.4.3.el7
kernel-abi-whitelists-3.10.0-1062.4.3.el7
164050 - Oracle Enterprise Linux ELSA-2019-3834 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ELSA-2019-3834

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

Fedora Core 29
libmp4v2-2.1.0-0.19.trunkREV507.fc29

195825 - Fedora Linux 29 FEDORA-2019-6469ad8129 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
FEDORA-2019-6469ad8129

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/2019/11/?count=200&page=1
195830 - Fedora Linux 31 FEDORA-2019-7a06c0e6b4 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
FEDORA-2019-7a06c0e6b4

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/2019/11/?count=200&page=1

Fedora Core 31
gd-2.2.5-10.fc31

195833 - Fedora Linux 29 FEDORA-2019-865bb16900 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
FEDORA-2019-865bb16900

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/2019/11/?count=200&page=2

Fedora Core 29
xen-4.11.2-2.fc29

195839 - Fedora Linux 31 FEDORA-2019-d53d4a79ac Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
FEDORA-2019-d53d4a79ac

Observation
Updates often remEDIATE critical security problems that should be quickly addressed.
Fedora Core 31
libmpv2-2.1.0-0.19.trunkREV507.fc31

195843 - Fedora Linux 30 FEDORA-2019-1030f4816a Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
FEDORA-2019-1030f4816a

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/2019/11/?count=200&page=1

Fedora Core 30
libmpv2-2.1.0-0.19.trunkREV507.fc30

195855 - Fedora Linux 30 FEDORA-2019-17f42f585a Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
FEDORA-2019-17f42f585a

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/2019/11/?count=200&page=1

Fedora Core 30
ghostscript-9.27-2.fc30

196536 - Red Hat Enterprise Linux RHSA-2019-3888 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-14869

----------
Description
The scan detected that the host is missing the following update:
RHSA-2019-3888

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


RHEL7D
x86_64
libgs-9.25-2.el7_7.3
ghostscript-debuginfo-9.25-2.el7_7.3
ghostscript-cups-9.25-2.el7_7.3
libgs-devel-9.25-2.el7_7.3
ghostscript-9.25-2.el7_7.3
ghostscript-gtk-9.25-2.el7_7.3

noarch
ghostscript-doc-9.25-2.el7_7.3

RHEL7S
noarch
ghostscript-doc-9.25-2.el7_7.3

x86_64
libgs-9.25-2.el7_7.3
ghostscript-debuginfo-9.25-2.el7_7.3
ghostscript-cups-9.25-2.el7_7.3
libgs-devel-9.25-2.el7_7.3
ghostscript-9.25-2.el7_7.3
ghostscript-gtk-9.25-2.el7_7.3

RHEL7WS
x86_64
libgs-9.25-2.el7_7.3
ghostscript-debuginfo-9.25-2.el7_7.3
ghostscript-cups-9.25-2.el7_7.3
libgs-devel-9.25-2.el7_7.3
ghostscript-9.25-2.el7_7.3
ghostscript-gtk-9.25-2.el7_7.3

noarch
ghostscript-doc-9.25-2.el7_7.3

196537 - Red Hat Enterprise Linux RHSA-2019-3895 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-14287

Description
The scan detected that the host is missing the following update:
RHSA-2019-3895

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


RHEL6_5S
x86_64
sudo-devel-1.8.6p3-12.el6_5.2
sudo-debuginfo-1.8.6p3-12.el6_5.2
sudo-1.8.6p3-12.el6_5.2

**25810 - Cisco Adaptive Security Appliance Software SIP Inspection Denial Of Service Vulnerability (cisco-sa-20191002-asa-ftd-sip-dos)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2019-12678

**Description**

A vulnerability is present in some versions of Cisco ASA Software.

**Observation**

Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco ASA Software. The flaw is due to improper parsing of Session Initiation Protocol(SIP) messages. Successful exploitation could allow an unauthenticated remote attacker to cause a denial of service condition on the target system.

**195829 - Fedora Linux 30 FEDORA-2019-460ad648e7 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium

**Description**

The scan detected that the host is missing the following update:
FEDORA-2019-460ad648e7

**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/2019/11/?count=200&page=2

Fedora Core 30

samba-4.10.10-0.fc30

**25752 - Cisco Adaptive Security Appliance Software WebVPN CPU Denial Of Service Vulnerability (cisco-sa-20191002-asa-ftd-dos)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2019-12698
A vulnerability is present in some versions of Cisco ASA Software.

Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco ASA Software. The flaw lies in handling multiple WebVPN HTTP page load requests. Successful exploitation could allow an unauthenticated remote attacker to cause a denial of service condition on the target system.

### 131476 - Debian Linux 10.0, 9.0 DSA-4571-1 Update Is Not Installed

**Category:** SSH Module -> NonIntrusive -> Debian Patches and Hotfixes  
**Risk Level:** Medium  

**Description**  
The scan detected that the host is missing the following update:  
DSA-4571-1

**Observation**  
Updates often remediate critical security problems that should be quickly addressed.  
For more information see:  
http://www.debian.org/security/2019/dsa-4571

Debian 9.0  
all  
thunderbird_1:68.2.2-1~deb9u1

Debian 10.0  
all  
thunderbird_1:68.2.2-1~deb10u1

### 171170 - Amazon Linux AMI ALAS-2019-1318 Update Is Not Installed

**Category:** SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes  
**Risk Level:** Medium  
**CVE:** CVE-2019-11135, CVE-2019-11139

**Description**  
The scan detected that the host is missing the following update:  
ALAS-2019-1318

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

Amazon Linux AMI  
x86_64  
kernel-debuginfo-common-x86_64-4.14.152-98.182.amzn1
195842 - Fedora Linux 29 FEDORA-2019-703e299870 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
FEDORA-2019-703e299870

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/2019/11/?count=200&page=2

Fedora Core 29
samba-4.9.15-0.fc29

195850 - Fedora Linux 30 FEDORA-2019-ec04c34768 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium

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/2019/11/?count=200&page=2

Fedora Core 30
libssh2-1.9.0-3.fc30

195858 - Fedora Linux 30 FEDORA-2019-45a744b873 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
FEDORA-2019-45a744b873

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/2019/11/?count=200&page=2

Fedora Core 30
thunderbird-enigmail-2.1.3-4.fc30

25762 - Cisco NX-OS Software Remote Management Memory Leak Denial Of Service Vulnerability (cisco-sa-20190828-nxos-memleak-dos)
Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2019-1965

Description
A vulnerability is present in some versions of Cisco NX-OS Software.

Observation
Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the Virtual Shell (VSH) session management of Cisco NX-OS Software. Successful exploitation could allow a remote attacker to cause a denial of service condition.

131473 - Debian Linux 9.0 DSA-4574-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
Description
The scan detected that the host is missing the following update:
DSA-4574-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2019/dsa-4574

Debian 9.0
all
redmine_3.3.1-4+deb9u3

131475 - Debian Linux 10.0 DSA-4570-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-11779

Description
The scan detected that the host is missing the following update:
DSA-4570-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2019/dsa-4570

Debian 10.0
all
mosquitto_1.5.7-1+deb10u1

183135 - FreeBSD GNU cpio Multiple Vulnerabilities (f59af308-07f3-11ea-8c56-f8b156b6dcc8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
GNU cpio -- multiple vulnerabilities (f59af308-07f3-11ea-8c56-f8b156b6dcc8)

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

Affected packages:
cpio < 2.13

195831 - Fedora Linux 31 FEDORA-2019-7841e28c1b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: FEDORA-2019-7841e28c1b

Description
The scan detected that the host is missing the following update:
FEDORA-2019-7841e28c1b

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.fedorahosted.org/bugzilla/show_bug.cgi?id=195831

Affected packages:
gcc < 7.3.1
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-16707

Description
The scan detected that the host is missing the following update:
FEDORA-2019-7841e28c1b

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/2019/11/?count=200&page=1

Fedora Core 31
hunspell-1.7.0-4.fc31

195836 - Fedora Linux 31 FEDORA-2019-67ff247aea Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
FEDORA-2019-67ff247aea

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/2019/11/?count=200&page=2

Fedora Core 31
djvulibre-3.5.27-16.fc31

195840 - Fedora Linux 30 FEDORA-2019-b217f90c2a Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
FEDORA-2019-b217f90c2a

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/2019/11/?count=200&page=1
Fedora Core 30

djvulibre-3.5.27-15.fc30

**195847 - Fedora Linux 30 FEDORA-2019-2bdcccee3c Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  

**Description**
The scan detected that the host is missing the following update:  
FEDORA-2019-2bdcccee3c

**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/2019/11/?count=200&page=2

Fedora Core 30

wpa_supplicant-2.8-3.fc30

**195848 - Fedora Linux 29 FEDORA-2019-7ca378f076 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  

**Description**
The scan detected that the host is missing the following update:  
FEDORA-2019-7ca378f076

**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/2019/11/?count=200&page=1

Fedora Core 29

djvulibre-3.5.27-14.fc29

**89051 - Slackware Linux 14.2 SSA:2019-320-01 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes  
Risk Level: Low  

**Description**
The scan detected that the host is missing the following update:  
SSA:2019-320-01
Observation
Updates often remediate critical security problems that should be quickly addressed. For more information see:


Slackware 14.2
i586
kernel-modules-4.4.202-i586-1
kernel-generic-4.4.202-i586-1
kernel-huge-4.4.202-i586-1

i686
kernel-modules-smp-4.4.202_smp-i686-1
kernel-huge-smp-4.4.202_smp-i686-1
kernel-generic-smp-4.4.202_smp-i686-1

noarch
kernel-source-4.4.202-noarch-1
kernel-source-4.4.202_smp-noarch-1

x86_64
kernel-huge-4.4.202-x86_64-1
kernel-modules-4.4.202-x86_64-1
kernel-generic-4.4.202-x86_64-1

131471 - Debian Linux 10.0, 9.0 DSA-4573-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low

Description
The scan detected that the host is missing the following update:
DSA-4573-1

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

http://www.debian.org/security/2019/dsa-4573

Debian 9.0
all
php-symfony-event-dispatcher_2.8.7+dfsg-1.3+deb9u3
php-symfony-phpunit-bridge_2.8.7+dfsg-1.3+deb9u3
php-symfony-dependency-injection_2.8.7+dfsg-1.3+deb9u3
php-symfony-templating_2.8.7+dfsg-1.3+deb9u3
php-symfony-security-http_2.8.7+dfsg-1.3+deb9u3
php-symfony-class-loader_2.8.7+dfsg-1.3+deb9u3
php-symfony-monolog-bridge_2.8.7+dfsg-1.3+deb9u3
php-symfony-security_2.8.7+dfsg-1.3+deb9u3
php-symfony-security-guard_2.8.7+dfsg-1.3+deb9u3
php-symfony-proxy-manager-bridge_2.8.7+dfsg-1.3+deb9u3
php-symfony-security-csrf_2.8.7+dfsg-1.3+deb9u3
php-symfony-routing_2.8.7+dfsg-1.3+deb9u3
php-symfony-security-bundle_2.8.7+dfsg-1.3+deb9u3
php-symfony-translation_2.8.7+dfsg-1.3+deb9u3
php-symfony-security-bundle_3.4.22+dfsg-2+deb10u1
php-symfony-doctrine-bridge_3.4.22+dfsg-2+deb10u1
php-symfony-class-loader_3.4.22+dfsg-2+deb10u1
php-symfony-console_3.4.22+dfsg-2+deb10u1
php-symfony-workflow_3.4.22+dfsg-2+deb10u1
php-symfony-web-profiler-bundle_3.4.22+dfsg-2+deb10u1
php-symfony-process_3.4.22+dfsg-2+deb10u1
php-symfony-security-http_3.4.22+dfsg-2+deb10u1
php-symfony-debug_3.4.22+dfsg-2+deb10u1
php-symfony-twig-bridge_3.4.22+dfsg-2+deb10u1
php-symfony-proxy-manager-bridge_3.4.22+dfsg-2+deb10u1
php-symfony-http-foundation_3.4.22+dfsg-2+deb10u1
php-symfony-web-link_3.4.22+dfsg-2+deb10u1
php-symfony-options-resolver_3.4.22+dfsg-2+deb10u1
php-symfony-dom-crawler_3.4.22+dfsg-2+deb10u1
php-symfony-browser-kit_3.4.22+dfsg-2+deb10u1
php-symfony-expression-language_3.4.22+dfsg-2+deb10u1
php-symfony-event-dispatcher_3.4.22+dfsg-2+deb10u1
php-symfony-monolog-bridge_3.4.22+dfsg-2+deb10u1
php-symfony-phpunit-bridge_3.4.22+dfsg-2+deb10u1
php-symfony-finder_3.4.22+dfsg-2+deb10u1
php-symfony-translation_3.4.22+dfsg-2+deb10u1
php-symfony-cache_3.4.22+dfsg-2+deb10u1
php-symfony-dependency-injection_3.4.22+dfsg-2+deb10u1
php-symfony-lock_3.4.22+dfsg-2+deb10u1
php-symfony-stopwatch_3.4.22+dfsg-2+deb10u1
php-symfony-validator_3.4.22+dfsg-2+deb10u1
php-symfony-security-core_3.4.22+dfsg-2+deb10u1
php-symfony-security_3.4.22+dfsg-2+deb10u1
php-symfony-asset_3.4.22+dfsg-2+deb10u1

131472 - Debian Linux 10.0, 9.0 DSA-4569-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-14869

Description
The scan detected that the host is missing the following update:
DSA-4569-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2019/dsa-4569

Debian 9.0
all
ghostscript_9.26a~dfsg-0+deb9u6

Debian 10.0
all
ghostscript_9.27~dfsg-2+deb10u3

131474 - Debian Linux 10.0, 9.0 DSA-4568-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3466

Description
The scan detected that the host is missing the following update:
DSA-4568-1

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

http://www.debian.org/security/2019/dsa-4568

Debian 9.0
all
postgresql-common_181+deb9u3

Debian 10.0
all
postgresql-common_200+deb10u3

183134 - FreeBSD libidn2 Roundtrip Check Vulnerability (f04f840d-0840-11ea-8d66-75d3253ef913)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-12290

Description
The scan detected that the host is missing the following update:
libidn2 -- roundtrip check vulnerability (f04f840d-0840-11ea-8d66-75d3253ef913)

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


Affected packages:
libidn2 < 2.3.0

183136 - FreeBSD drm graphics drivers Local Privilege Escalation And Denial Of Service (ecb7fdec-0b82-11ea-874d-0c9d925bbbc0)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low

Description
The scan detected that the host is missing the following update:
drm graphics drivers -- Local privilege escalation and denial of service (ecb7fdec-0b82-11ea-874d-0c9d925bbbc0)

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
Affected packages:
drm-current-kmod < 4.16.g20191120
drm-devel-kmod < 5.0.g20191120
drm-fbsd12.0-kmod < 4.16.g20191120

183137 - FreeBSD squid Vulnerable To HTTP Digest Authentication (620685d6-0aa3-11ea-9673-4c72b94353b5)
Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-18679

Description
The scan detected that the host is missing the following update:
squid -- Vulnerable to HTTP Digest Authentication (620685d6-0aa3-11ea-9673-4c72b94353b5)

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/620685d6-0aa3-11ea-9673-4c72b94353b5.html

Affected packages:
squid < 4.9

195821 - Fedora Linux 29 FEDORA-2019-be01267416 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3465

Description
The scan detected that the host is missing the following update:
FEDORA-2019-be01267416

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/2019/11/?count=200&page=2

Fedora Core 29
php-robrichards-xmlseclibs3-3.0.4-1.fc29

195822 - Fedora Linux 31 FEDORA-2019-6cdb10aa59 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-14869

Description
The scan detected that the host is missing the following update:
FEDORA-2019-6cdb10aa59

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/2019/11/?count=200&page=1

Fedora Core 31
ghostscript-9.27-2.fc31

195823 - Fedora Linux 30 FEDORA-2019-ec8719a21c Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3465

Description
The scan detected that the host is missing the following update:
FEDORA-2019-ec8719a21c

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/2019/11/?count=200&page=2

Fedora Core 30
php-robrichards-xmlseclibs3-3.0.4-1.fc30

195824 - Fedora Linux 29 FEDORA-2019-81f61cdceb Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3465

Description
The scan detected that the host is missing the following update:
FEDORA-2019-81f61cdceb

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/2019/11/?count=200&page=2

Fedora Core 29
php-robrichards-xmlseclibs-2.1.1-1.fc29

195826 - Fedora Linux 31 FEDORA-2019-7c3227fea5 Update Is Not Installed
Description
The scan detected that the host is missing the following update:
FEDORA-2019-7c3227fea5

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/2019/11/?count=200&page=1

Fedora Core 31
limnoria-20191109-2.fc31

195827 - Fedora Linux 29 FEDORA-2019-65509aac53 Update Is Not Installed

Description
The scan detected that the host is missing the following update:
FEDORA-2019-65509aac53

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/2019/11/?count=200&page=2

Fedora Core 29
wpa_supplicant-2.7-2.fc29

195828 - Fedora Linux 29 FEDORA-2019-ba59b4b9f1 Update Is Not Installed

Description
The scan detected that the host is missing the following update:
FEDORA-2019-ba59b4b9f1

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/2019/11/?count=200&page=1
Fedora Core 29

java-1.8.0-openjdk-aarch32-1.8.0.232.b09-1.fc29

195832 - Fedora Linux 31 FEDORA-2019-eee0d6c6f8 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-2201

Description
The scan detected that the host is missing the following update:
FEDORA-2019-eee0d6c6f8

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/2019/11/?count=200&page=1

Fedora Core 31

libjpeg-turbo-2.0.2-5.fc31

195834 - Fedora Linux 30 FEDORA-2019-e8695f5e6c 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-e8695f5e6c

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/2019/11/?count=200&page=1

Fedora Core 30

java-1.8.0-openjdk-aarch32-1.8.0.232.b09-1.fc30

195835 - Fedora Linux 30 FEDORA-2019-4213e37211 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low

Description
The scan detected that the host is missing the following update:
FEDORA-2019-4213e37211
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/2019/11/?count=200&page=2

Fedora Core 30

webkit2gtk3-2.26.2-1.fc30

195837 - Fedora Linux 31 FEDORA-2019-376ec5c107 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low

Description
The scan detected that the host is missing the following update:
FEDORA-2019-376ec5c107

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/2019/11/?count=200&page=1

Fedora Core 31

xen-4.12.1-6.fc31

195838 - Fedora Linux 29 FEDORA-2019-742811fc22 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-19010

Description
The scan detected that the host is missing the following update:
FEDORA-2019-742811fc22

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/2019/11/?count=200&page=1

Fedora Core 29

limnoria-20191109-2.fc29

195841 - Fedora Linux 31 FEDORA-2019-fa0c4b0674 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low

Description
The scan detected that the host is missing the following update:
FEDORA-2019-fa0c4b0674

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/2019/11/?count=200&page=2

Fedora Core 31

webkit2gtk3-2.26.2-1.fc31

195844 - Fedora Linux 30 FEDORA-2019-db2d7b1c80 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-db2d7b1c80

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/2019/11/?count=200&page=2

Fedora Core 30

freetds-1.1.20-1.fc30

195845 - Fedora Linux 31 FEDORA-2019-c0da3238ae 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-c0da3238ae

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/2019/11/?count=200&page=2

Fedora Core 31
195846 - Fedora Linux 29 FEDORA-2019-8508d74523 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low

Description
The scan detected that the host is missing the following update:
FEDORA-2019-8508d74523

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/2019/11/?count=200&page=2

Fedora Core 29

chromium-78.0.3904.87-1.fc29

195849 - Fedora Linux 30 FEDORA-2019-dc90bf093b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3465

Description
The scan detected that the host is missing the following update:
FEDORA-2019-dc90bf093b

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/2019/11/?count=200&page=2

Fedora Core 30

php-robrichards-xmlseclibs-2.1.1-1.fc30

195851 - Fedora Linux 30 FEDORA-2019-2fa7552273 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
Description
The scan detected that the host is missing the following update:
FEDORA-2019-2fa7552273

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/2019/11/?count=200&page=2

Fedora Core 30
chromium-78.0.3904.87-1.fc30

195852 - Fedora Linux 31 FEDORA-2019-c170ad0c6b 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-c170ad0c6b

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/2019/11/?count=200&page=2

Fedora Core 31
java-1.8.0-openjdk-aarch32-1.8.0.232.b09-1.fc31

195853 - Fedora Linux 29 FEDORA-2019-cf742c353a 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-cf742c353a

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/2019/11/?count=200&page=1

Fedora Core 29
freetds-1.1.20-1.fc29

195854 - Fedora Linux 31 FEDORA-2019-73d0fe1d15 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3465

Description
The scan detected that the host is missing the following update:
FEDORA-2019-73d0fe1d15

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/2019/11/?count=200&page=2

Fedora Core 31

php-robrichards-xmlseclibs-2.1.1-1.fc31

195856 - Fedora Linux 31 FEDORA-2019-9a960c8a98 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-3465

Description
The scan detected that the host is missing the following update:
FEDORA-2019-9a960c8a98

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/2019/11/?count=200&page=2

Fedora Core 31

php-robrichards-xmlseclibs3-3.0.4-1.fc31

195857 - Fedora Linux 31 FEDORA-2019-b67929609d 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-b67929609d

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/2019/11/?count=200&page=2

Fedora Core 31
freetds-1.1.20-1.fc31

**195859 - Fedora Linux 31 FEDORA-2019-f454c7a118 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-12290

**Description**
The scan detected that the host is missing the following update:
FEDORA-2019-f454c7a118

**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/2019/11/?count=200&page=1

Fedora Core 31
libidn2-2.3.0-1.fc31

**195860 - Fedora Linux 30 FEDORA-2019-789f4e5494 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-19010

**Description**
The scan detected that the host is missing the following update:
FEDORA-2019-789f4e5494

**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/2019/11/?count=200&page=1

Fedora Core 30
limnoria-20191109-2.fc30

**148537 - SuSE Linux 15.0 openSUSE-SU-2019:2505-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Low
Description
The scan detected that the host is missing the following update:
openSUSE-SU-2019:2505-1

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

SuSE Linux 15.0
x86_64
qemu-arm-2.11.2-lp150.7.28.1
qemu-block-gluster-2.11.2-lp150.7.28.1
qemu-ppc-debuginfo-2.11.2-lp150.7.28.1
qemu-guest-agent-2.11.2-lp150.7.28.1
qemu-extra-debuginfo-2.11.2-lp150.7.28.1
qemu-kvm-2.11.2-lp150.7.28.1
qemu-block-rbd-debuginfo-2.11.2-lp150.7.28.1
qemu-block-ssh-2.11.2-lp150.7.28.1
qemu-tools-debuginfo-2.11.2-lp150.7.28.1
qemu-s390-2.11.2-lp150.7.28.1
qemu-s390-debuginfo-2.11.2-lp150.7.28.1
qemu-block-rbd-2.11.2-lp150.7.28.1
qemu-arm-debuginfo-2.11.2-lp150.7.28.1
qemu-ppc-2.11.2-lp150.7.28.1
qemu-x86-2.11.2-lp150.7.28.1
qemu-block-iscsi-debuginfo-2.11.2-lp150.7.28.1
qemu-block-ssh-debuginfo-2.11.2-lp150.7.28.1
qemu-guest-agent-debuginfo-2.11.2-lp150.7.28.1
qemu-extra-2.11.2-lp150.7.28.1
qemu-x86-debuginfo-2.11.2-lp150.7.28.1
qemu-block-dmg-2.11.2-lp150.7.28.1
qemu-lang-2.11.2-lp150.7.28.1
qemu-block-curl-debuginfo-2.11.2-lp150.7.28.1
qemu-block-dmg-debuginfo-2.11.2-lp150.7.28.1
qemu-debuginfo-2.11.2-lp150.7.28.1
qemu-debugsource-2.11.2-lp150.7.28.1
qemu-block-iscsi-2.11.2-lp150.7.28.1
qemu-block-gluster-debuginfo-2.11.2-lp150.7.28.1
qemu-block-curl-2.11.2-lp150.7.28.1
qemu-tools-2.11.2-lp150.7.28.1
qemu-ksm-2.11.2-lp150.7.28.1
qemu-2.11.2-lp150.7.28.1
noarch
qemu-seabios-1.11.0-lp150.7.28.1
qemu-ipxe-1.0.0+-lp150.7.28.1
qemu-vgabios-1.11.0-lp150.7.28.1
qemu-sgabios-8-lp150.7.28.1

**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.

96062 - Red Hat Enterprise Linux RHSA-2018-1737 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High

Update Details
CVE is updated FASLScript is updated

**96060 - Red Hat Enterprise Linux RHSA-2018-1700 Update Is Not Installed**

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

Update Details
CVE is updated FASLScript is updated

**96063 - Red Hat Enterprise Linux RHSA-2018-1707 Update Is Not Installed**

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

Update Details
CVE is updated FASLScript is updated

**96061 - Red Hat Enterprise Linux RHSA-2018-1722 Update Is Not Installed**

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

Update Details
CVE is updated FASLScript is updated

**96059 - Red Hat Enterprise Linux RHSA-2018-1638 Update Is Not Installed**

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

Update Details
CVE is updated FASLScript is updated
HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com
Multi-National Phone Support available here:
http://www.mcafee.com/us/about/contact/index.html
Non-US customers - Select your country from the list of Worldwide Offices.

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