2019-MAY-15
FSL version 7.6.111

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

147916 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:1388-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11627

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1388-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00085.html

SuSE Linux 15.0
x86_64
signing-party-debuginfo-2.7-lp150.5.1
signing-party-2.7-lp150.5.1
signing-party-debugsource-2.7-lp150.5.1

SuSE Linux 42.3
noarch
signing-party-2.1-10.3.1

186698 - Ubuntu Linux 19.04 USN-3979-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11683, CVE-2019-1999, CVE-2019-3874, CVE-2019-3882, CVE-2019-3887, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
USN-3979-1

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-May/004895.html

Ubuntu 19.04

linux-image-kvm_5.0.0.1006.6
linux-image-virtual_5.0.0.15.16
linux-image-aws_5.0.0.1006.6
linux-image-gke_5.0.0.1006.6
linux-image-5.0.0-1006-azure_5.0.0-1006.6
linux-image-generic-lpae_5.0.0.15.16
linux-image-azure_5.0.0.1006.6
linux-image-raspi2_5.0.0.1008.5
linux-image-5.0.0-1006-aws_5.0.0-1006.6
linux-image-5.0.0-1008-raspi2_5.0.0-1008.8
linux-image-5.0.0-1006-kvm_5.0.0-1006.6
linux-image-generic_5.0.0.15.16
linux-image-gcp_5.0.0.1006.6
linux-image-5.0.0-15-lowlatency_5.0.0-15.16
linux-image-5.0.0-1006-gcp_5.0.0-1006.6
linux-image-5.0.0-15-generic-lpae_5.0.0-15.16
linux-image-5.0.0-15-generic_5.0.0-15.16
linux-image-lowlatency_5.0.0.15.16

195154 - Fedora Linux 30 FEDORA-2019-5b76e711b3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11683, CVE-2019-3900

Description

The scan detected that the host is missing the following update:
FEDORA-2019-5b76e711b3

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/2019/5/?count=200&page=3

Fedora Core 30

kernel-5.0.13-300.fc30
kernel-tools-5.0.12-300.fc30

25140 - (MSPT-May2019) Microsoft Guidance To Mitigate Microarchitectural Data Sampling Vulnerabilities (ADV190013)

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

Risk Level: High

CVE: CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130

Description

Multiple vulnerabilities are present in some versions of Microsoft Windows could lead to information disclosure.

Observation

Multiple vulnerabilities are present in some versions of Microsoft Windows could lead to information disclosure.

The flaws lie in unspecified component. Successful exploitation could allow a local user to disclose sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

25179 - (APSB19-18) Multiple Vulnerabilities In Adobe Acrobat And Reader

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

Risk Level: High

CVE: CVE-2019-7140, CVE-2019-7141, CVE-2019-7142, CVE-2019-7143, CVE-2019-7144, CVE-2019-7145, CVE-2019-7758, CVE-2019-7759, CVE-2019-7760, CVE-2019-7761, CVE-2019-7762, CVE-2019-7763, CVE-2019-7764, CVE-2019-7765, CVE-2019-7766, CVE-2019-7767, CVE-2019-7768, CVE-2019-7769, CVE-2019-7770, CVE-2019-7771, CVE-2019-7772, CVE-2019-7773, CVE-2019-7774, CVE-2019-7775, CVE-2019-7776, CVE-2019-7777, CVE-2019-7778, CVE-2019-7779, CVE-2019-7780, CVE-2019-7781, CVE-2019-7782, CVE-2019-7783, CVE-2019-7784, CVE-2019-7785, CVE-2019-7786, CVE-2019-7787, CVE-2019-7788, CVE-2019-7789, CVE-2019-7790, CVE-2019-7791, CVE-2019-7792, CVE-2019-7793, CVE-2019-7794, CVE-2019-7795, CVE-2019-7796, CVE-2019-7797, CVE-2019-7798, CVE-2019-7799, CVE-2019-7800, CVE-2019-7801, CVE-2019-7802, CVE-2019-7803, CVE-2019-7804, CVE-2019-7805, CVE-2019-7806, CVE-2019-7807, CVE-2019-7808, CVE-2019-7809, CVE-2019-7810, CVE-2019-7811, CVE-2019-7812, CVE-2019-7813, CVE-2019-7814, CVE-2019-7817, CVE-2019-7818, CVE-2019-7819, CVE-2019-7820, CVE-2019-7821, CVE-2019-7822, CVE-2019-7823, CVE-2019-7824, CVE-2019-7825, CVE-2019-7826, CVE-2019-7827, CVE-2019-7828, CVE-2019-7829, CVE-2019-7830, CVE-2019-7831, CVE-2019-7832, CVE-2019-7833, CVE-2019-7834, CVE-2019-7835, CVE-2019-7836, CVE-2019-7841

Description

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat.

Observation

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

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat. The flaws lie in undetermined components. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

The update provided by Adobe bulletin APSB19-18 resolves these issues.

25180 - (APSB19-26) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2019-7837

Description

A vulnerability is present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

A vulnerability is present in some versions of Adobe Flash Player. The flaw lies in the Adobe Flash Player Runtime. Successful exploitation could allow an attacker to execute remote code and take control of the affected system.

25141 - (MSPT-May2019) Microsoft Browsers Scripting Engine Remote Code Execution (CVE-2019-0911)

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

Risk Level: High

CVE: CVE-2019-0911

Description

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

Observation

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25142 - (MSPT-May2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0912)

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

Risk Level: High

CVE: CVE-2019-0912

Description

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

Observation

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

The flaw lies in the Chakra component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25143 - (MSPT-May2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0915)

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

Risk Level: High

CVE: CVE-2019-0915

Description

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

Observation

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

The flaw lies in the Chakra component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25103 - (MSPT-May2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0917)

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

Risk Level: High

CVE: CVE-2019-0917

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution

of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25132 - (MSPT-May2019) Microsoft Azure DevOps Server and Team Foundation Server Cross-site Scripting (CVE-2019-0979)

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

Risk Level: High

CVE: CVE-2019-0979

Description

A vulnerability in some versions of Microsoft Azure DevOps Server and Team Foundation Server could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Azure DevOps Server and Team Foundation Server could lead to remote code execution.

The flaw is due to improper handling of a specially crafted payload. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

25135 - (MSPT-May2019) Microsoft SharePoint Server Remote Code Execution (CVE-2019-0952)

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

Risk Level: High

CVE: CVE-2019-0952

Description

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

Observation

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

The flaw lies in the asp.net web controls component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

25145 - (MSPT-May2019) Microsoft Internet Explorer Security Feature Bypass (CVE-2019-0995)

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

Risk Level: High

CVE: CVE-2019-0995

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to security feature bypass.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to security feature bypass.

The flaw lies in urlmon.dll. Successful exploitation could allow a remote attacker to bypass certain security restrictions. The exploit requires the user to open a vulnerable website, email or document.

25147 - (MSPT-May2019) Microsoft .NET Core Denial of Service (CVE-2019-0980)

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

Risk Level: High

CVE: CVE-2019-0980

Description

A vulnerability in some versions of Microsoft .NET Core could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft .NET Core could lead to a denial of service.

The flaw is due to improper handling of web requests. Successful exploitation by a remote attacker could result in a denial of service condition.

25148 - (MSPT-May2019) Microsoft .Net Framework and .Net Core Denial of Service (CVE-2019-0981)

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

Risk Level: High

CVE: CVE-2019-0981

Description

A vulnerability in some versions of Microsoft .NET Core could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft .NET Core could lead to a denial of service.

The flaw is due to improper handling of web requests. Successful exploitation by a remote attacker could result in a denial of service condition.

25149 - (MSPT-May2019) Microsoft .NET Core Denial of Service (CVE-2019-0982)

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

Risk Level: High

CVE: CVE-2019-0982

Description

A vulnerability in some versions of Microsoft .NET Core could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft .NET Core could lead to a denial of service.

The flaw is due to improper handling of web requests. Successful exploitation by a remote attacker could result in a denial of service condition.

25152 - (MSPT-May2019) Microsoft .NET Framework and Core Denial of Service (CVE-2019-0820)

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

Risk Level: High

CVE: CVE-2019-0820

Description

A vulnerability in some versions of Microsoft .NET Framework and .NET Core could lead to denial of service.

Observation

A vulnerability in some versions of Microsoft .NET Framework and .NET Core could lead to denial of service.

The flaw is due to improper handling of RegEx strings. Successful exploitation by a remote attacker could result in a denial of service condition.

25154 - (MSPT-May2019) Microsoft Browser Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0918)

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

Risk Level: High

CVE: CVE-2019-0918

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25157 - (MSPT-May2019) Microsoft Internet Explorer Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0929)

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

Risk Level: High

CVE: CVE-2019-0929

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25158 - (MSPT-May2019) Microsoft Browser Improperly Accesses Objects in Memory Remote Code Execution (CVE-2019-0940)

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

Risk Level: High

CVE: CVE-2019-0940

Description

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

Observation

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

The flaw lies due to improperly accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25160 - (MSPT-May2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0925)

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

Risk Level: High

CVE: CVE-2019-0925

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25161 - (MSPT-May2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0924)

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

Risk Level: High

CVE: CVE-2019-0924

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25162 - (MSPT-May2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0923)

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

Risk Level: High

CVE: CVE-2019-0923

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25163 - (MSPT-May2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0922)

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

Risk Level: High

CVE: CVE-2019-0922

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25164 - (MSPT-May2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0927)

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

Risk Level: High

CVE: CVE-2019-0927

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25165 - (MSPT-May2019) Microsoft Edge Improperly Accesses Objects in Memory Remote Code Execution (CVE-2019-0926)

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

Risk Level: High

CVE: CVE-2019-0926

Description

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

Observation

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

The flaw lies due to improperly accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25167 - (MSPT-May2019) Microsoft Word Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0953)

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

Risk Level: High

CVE: CVE-2019-0953

Description

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

Observation

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

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25168 - (MSPT-May2019) Microsoft Office Connectivity Engine Remote Code Execution (CVE-2019-0947)

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

Risk Level: High

CVE: CVE-2019-0947

Description

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

Observation

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

The flaw lies in the connectivity engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25169 - (MSPT-May2019) Microsoft Office Connectivity Engine Remote Code Execution (CVE-2019-0946)

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

Risk Level: High

CVE: CVE-2019-0946

Description

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

Observation

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

The flaw lies in the connectivity engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25170 - (MSPT-May2019) Microsoft Office Connectivity Engine Remote Code Execution (CVE-2019-0945)

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

Risk Level: High

CVE: CVE-2019-0945

Description

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

Observation

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

The flaw lies in the connectivity engine. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

132503 - Oracle VM OVMSA-2019-0018 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0018

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2019-May/000940.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-124.26.12.el6uek
kernel-uek-4.1.12-124.26.12.el6uek

132504 - Oracle VM OVMSA-2019-0016 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0016

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2019-May/000939.html

OVM3.4
x86_64
xen-4.4.4-222.0.4.el6

xen-tools-4.4.4-222.0.4.el6

147913 - SuSE SLES 12 SP4 SUSE-SU-2019:1242-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16880, CVE-2019-11091, CVE-2019-3882, CVE-2019-9003, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1242-1

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-May/005451.html

SuSE SLES 12 SP4
x86_64
kernel-azure-debugsource-4.12.14-6.12.1
kernel-syms-azure-4.12.14-6.12.1
kernel-azure-base-4.12.14-6.12.1
kernel-azure-base-debuginfo-4.12.14-6.12.1
kernel-azure-debuginfo-4.12.14-6.12.1
kernel-azure-4.12.14-6.12.1
kernel-azure-devel-4.12.14-6.12.1

noarch
kernel-devel-azure-4.12.14-6.12.1
kernel-source-azure-4.12.14-6.12.1

147914 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:1243-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1243-1

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-May/005461.html

SuSE SLED 12 SP3
x86_64
qemu-debugsource-2.9.1-6.34.1
qemu-kvm-2.9.1-6.34.1
qemu-tools-debuginfo-2.9.1-6.34.1
qemu-tools-2.9.1-6.34.1
qemu-block-curl-debuginfo-2.9.1-6.34.1

qemu-2.9.1-6.34.1
qemu-x86-2.9.1-6.34.1
qemu-block-curl-2.9.1-6.34.1

noarch
qemu-ipxe-1.0.0+-6.34.1
qemu-sgabios-8-6.34.1
qemu-seabios-1.10.2-6.34.1
qemu-vgabios-1.10.2-6.34.1

SuSE SLES 12 SP3
noarch
qemu-ipxe-1.0.0+-6.34.1
qemu-sgabios-8-6.34.1
qemu-seabios-1.10.2-6.34.1
qemu-vgabios-1.10.2-6.34.1

x86_64
qemu-tools-2.9.1-6.34.1
qemu-2.9.1-6.34.1
qemu-kvm-2.9.1-6.34.1
qemu-block-ssh-2.9.1-6.34.1
qemu-block-curl-2.9.1-6.34.1
qemu-x86-debuginfo-2.9.1-6.34.1
qemu-guest-agent-2.9.1-6.34.1
qemu-block-ssh-debuginfo-2.9.1-6.34.1
qemu-block-curl-debuginfo-2.9.1-6.34.1
qemu-block-rbd-debuginfo-2.9.1-6.34.1
qemu-tools-debuginfo-2.9.1-6.34.1
qemu-lang-2.9.1-6.34.1
qemu-x86-2.9.1-6.34.1
qemu-debugsource-2.9.1-6.34.1
qemu-block-iscsi-debuginfo-2.9.1-6.34.1
qemu-guest-agent-debuginfo-2.9.1-6.34.1
qemu-block-iscsi-2.9.1-6.34.1
qemu-block-rbd-2.9.1-6.34.1

147915 - SuSE SLED 15 SUSE-SU-2019:1244-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16880, CVE-2019-11091, CVE-2019-3882, CVE-2019-9003, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1244-1

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-May/005458.html

SuSE SLED 15
x86_64
kernel-default-extra-debuginfo-4.12.14-150.17.1
kernel-default-extra-4.12.14-150.17.1

kernel-default-debuginfo-4.12.14-150.17.1
kernel-default-debugsource-4.12.14-150.17.1

147921 - SuSE Linux 42.3 openSUSE-SU-2019:1351-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19636, CVE-2018-19637, CVE-2018-19638, CVE-2018-19639, CVE-2018-19640

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1351-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00050.html

SuSE Linux 42.3
noarch
hostinfo-1.0.1-21.3.1

147922 - SuSE Linux 42.3 openSUSE-SU-2019:1373-1 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:
openSUSE-SU-2019:1373-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00070.html

SuSE Linux 42.3
i586
libopenssl1_0_0-debuginfo-1.0.2j-38.1
libopenssl1_0_0-hmac-1.0.2j-38.1
libopenssl-devel-1.0.2j-38.1
openssl-1.0.2j-38.1
openssl-debugsource-1.0.2j-38.1
openssl-cavs-debuginfo-1.0.2j-38.1
openssl-cavs-1.0.2j-38.1
libopenssl1_0_0-1.0.2j-38.1
openssl-debuginfo-1.0.2j-38.1

noarch
openssl-doc-1.0.2j-38.1

x86_64
libopenssl-devel-32bit-1.0.2j-38.1

openssl-debuginfo-1.0.2j-38.1
libopenssl1_0_0-hmac-32bit-1.0.2j-38.1
libopenssl-devel-1.0.2j-38.1
openssl-1.0.2j-38.1
openssl-cavs-debuginfo-1.0.2j-38.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-38.1
libopenssl1_0_0-hmac-1.0.2j-38.1
libopenssl1_0_0-1.0.2j-38.1
openssl-cavs-1.0.2j-38.1
libopenssl1_0_0-32bit-1.0.2j-38.1
openssl-debugsource-1.0.2j-38.1
libopenssl1_0_0-debuginfo-1.0.2j-38.1

147931 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1232-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11068

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1232-1

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-May/005448.html

SuSE SLED 12 SP3
x86_64
libxslt1-32bit-1.1.28-17.3.1
libxslt1-1.1.28-17.3.1
libxslt-debugsource-1.1.28-17.3.1
libxslt-tools-debuginfo-1.1.28-17.3.1
libxslt1-debuginfo-1.1.28-17.3.1
libxslt-tools-1.1.28-17.3.1
libxslt1-debuginfo-32bit-1.1.28-17.3.1

SuSE SLED 12 SP4
x86_64
libxslt1-32bit-1.1.28-17.3.1
libxslt1-1.1.28-17.3.1
libxslt-debugsource-1.1.28-17.3.1
libxslt-tools-debuginfo-1.1.28-17.3.1
libxslt1-debuginfo-1.1.28-17.3.1
libxslt-tools-1.1.28-17.3.1
libxslt1-debuginfo-32bit-1.1.28-17.3.1

SuSE SLES 12 SP4
x86_64
libxslt1-32bit-1.1.28-17.3.1
libxslt1-1.1.28-17.3.1
libxslt-debugsource-1.1.28-17.3.1
libxslt-tools-debuginfo-1.1.28-17.3.1
libxslt1-debuginfo-1.1.28-17.3.1
libxslt-tools-1.1.28-17.3.1
libxslt1-debuginfo-32bit-1.1.28-17.3.1

SuSE SLES 12 SP3
x86_64
libxslt1-32bit-1.1.28-17.3.1
libxslt1-1.1.28-17.3.1
libxslt-debugsource-1.1.28-17.3.1
libxslt-tools-debuginfo-1.1.28-17.3.1
libxslt1-debuginfo-1.1.28-17.3.1
libxslt-tools-1.1.28-17.3.1
libxslt1-debuginfo-32bit-1.1.28-17.3.1

147932 - SuSE Linux 15.0 openSUSE-SU-2019:1395-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10745, CVE-2019-10906, CVE-2019-8341

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1395-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00086.html

SuSE Linux 15.0
noarch
python2-Jinja2-2.10.1-lp150.2.3.1
python-Jinja2-vim-2.10.1-lp150.2.3.1
python-Jinja2-emacs-2.10.1-lp150.2.3.1
python3-Jinja2-2.10.1-lp150.2.3.1

147934 - SuSE Linux 42.3 openSUSE-SU-2019:1394-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11234, CVE-2019-11235

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1394-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00089.html

SuSE Linux 42.3
x86_64
freeradius-server-mysql-debuginfo-3.0.15-9.1
freeradius-server-ldap-3.0.15-9.1
freeradius-server-krb5-debuginfo-3.0.15-9.1
freeradius-server-libs-debuginfo-3.0.15-9.1

freeradius-server-sqlite-debuginfo-3.0.15-9.1
freeradius-server-perl-debuginfo-3.0.15-9.1
freeradius-server-python-debuginfo-3.0.15-9.1
freeradius-server-mysql-3.0.15-9.1
freeradius-server-krb5-3.0.15-9.1
freeradius-server-perl-3.0.15-9.1
freeradius-server-postgresql-3.0.15-9.1
freeradius-server-3.0.15-9.1
freeradius-server-postgresql-debuginfo-3.0.15-9.1
freeradius-server-utils-debuginfo-3.0.15-9.1
freeradius-server-ldap-debuginfo-3.0.15-9.1
freeradius-server-python-3.0.15-9.1
freeradius-server-libs-3.0.15-9.1
freeradius-server-devel-3.0.15-9.1
freeradius-server-doc-3.0.15-9.1
freeradius-server-sqlite-3.0.15-9.1
freeradius-server-debuginfo-3.0.15-9.1
freeradius-server-debugsource-3.0.15-9.1
freeradius-server-utils-3.0.15-9.1

147936 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1235-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1235-1

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-May/005459.html

SuSE SLED 12 SP3
x86_64
ucode-intel-20190507-13.41.1
ucode-intel-debugsource-20190507-13.41.1
ucode-intel-debuginfo-20190507-13.41.1

SuSE SLED 12 SP4
x86_64
ucode-intel-20190507-13.41.1
ucode-intel-debugsource-20190507-13.41.1
ucode-intel-debuginfo-20190507-13.41.1

SuSE SLES 12 SP4
x86_64
ucode-intel-20190507-13.41.1
ucode-intel-debugsource-20190507-13.41.1
ucode-intel-debuginfo-20190507-13.41.1

SuSE SLES 12 SP3
x86_64
ucode-intel-20190507-13.41.1
ucode-intel-debugsource-20190507-13.41.1

ucode-intel-debuginfo-20190507-13.41.1

147937 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:1196-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9116, CVE-2018-14349, CVE-2018-14350, CVE-2018-14351, CVE-2018-14352, CVE-2018-14353, CVE-2018-14354, CVE-2018-14355, CVE-2018-14356, CVE-2018-14357, CVE-2018-14358, CVE-2018-14359, CVE-2018-14360, CVE-2018-14361, CVE-2018-14362, CVE-2018-14363

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1196-1

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-May/005432.html

SuSE SLED 12 SP3
x86_64
mutt-debugsource-1.10.1-55.6.1
mutt-debuginfo-1.10.1-55.6.1
mutt-1.10.1-55.6.1

SuSE SLES 12 SP3
x86_64
mutt-debugsource-1.10.1-55.6.1
mutt-debuginfo-1.10.1-55.6.1
mutt-1.10.1-55.6.1

147938 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:1214-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000031

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1214-1

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-May/005433.html

SuSE SLES 12 SP3
noarch
jakarta-commons-fileupload-1.1.1-122.3.1
jakarta-commons-fileupload-javadoc-1.1.1-122.3.1

SuSE SLES 12 SP4
noarch
jakarta-commons-fileupload-1.1.1-122.3.1

jakarta-commons-fileupload-javadoc-1.1.1-122.3.1

147940 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1208-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10989, CVE-2018-8740

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1208-1

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-May/005442.html

SuSE SLED 12 SP3
x86_64
libsqlite3-0-3.8.10.2-9.6.1
sqlite3-debuginfo-3.8.10.2-9.6.1
sqlite3-debugsource-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-3.8.10.2-9.6.1
sqlite3-3.8.10.2-9.6.1
libsqlite3-0-32bit-3.8.10.2-9.6.1

SuSE SLED 12 SP4
x86_64
libsqlite3-0-3.8.10.2-9.6.1
sqlite3-debuginfo-3.8.10.2-9.6.1
sqlite3-debugsource-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-3.8.10.2-9.6.1
sqlite3-3.8.10.2-9.6.1
libsqlite3-0-32bit-3.8.10.2-9.6.1

SuSE SLES 12 SP4
x86_64
libsqlite3-0-3.8.10.2-9.6.1
sqlite3-debuginfo-3.8.10.2-9.6.1
sqlite3-debugsource-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-3.8.10.2-9.6.1
sqlite3-3.8.10.2-9.6.1
libsqlite3-0-32bit-3.8.10.2-9.6.1

SuSE SLES 12 SP3
x86_64
libsqlite3-0-3.8.10.2-9.6.1
sqlite3-debuginfo-3.8.10.2-9.6.1
sqlite3-debugsource-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.6.1
libsqlite3-0-debuginfo-3.8.10.2-9.6.1
sqlite3-3.8.10.2-9.6.1
libsqlite3-0-32bit-3.8.10.2-9.6.1

147942 - SuSE Linux 15.0 openSUSE-SU-2019:1341-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14779, CVE-2018-14780

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1341-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00046.html

SuSE Linux 15.0
x86_64
yubico-piv-tool-debuginfo-1.5.0-lp150.2.3.1
libykpiv-devel-1.5.0-lp150.2.3.1
libykcs11-1-debuginfo-1.5.0-lp150.2.3.1
yubico-piv-tool-1.5.0-lp150.2.3.1
libykcs11-devel-1.5.0-lp150.2.3.1
yubico-piv-tool-debugsource-1.5.0-lp150.2.3.1
libykpiv1-debuginfo-1.5.0-lp150.2.3.1
libykpiv1-1.5.0-lp150.2.3.1
libykcs11-1-1.5.0-lp150.2.3.1

147943 - SuSE Linux 15.0 openSUSE-SU-2019:1346-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11234, CVE-2019-11235

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1346-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00044.html

SuSE Linux 15.0
x86_64
freeradius-server-libs-3.0.16-lp150.2.3.1
freeradius-server-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-doc-3.0.16-lp150.2.3.1
freeradius-server-python-3.0.16-lp150.2.3.1
freeradius-server-utils-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-sqlite-3.0.16-lp150.2.3.1
freeradius-server-postgresql-3.0.16-lp150.2.3.1
freeradius-server-ldap-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-perl-3.0.16-lp150.2.3.1
freeradius-server-postgresql-debuginfo-3.0.16-lp150.2.3.1

freeradius-server-krb5-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-debugsource-3.0.16-lp150.2.3.1
freeradius-server-mysql-3.0.16-lp150.2.3.1
freeradius-server-ldap-3.0.16-lp150.2.3.1
freeradius-server-python-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-3.0.16-lp150.2.3.1
freeradius-server-utils-3.0.16-lp150.2.3.1
freeradius-server-devel-3.0.16-lp150.2.3.1
freeradius-server-perl-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-libs-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-sqlite-debuginfo-3.0.16-lp150.2.3.1
freeradius-server-krb5-3.0.16-lp150.2.3.1
freeradius-server-mysql-debuginfo-3.0.16-lp150.2.3.1

147945 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:1241-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16880, CVE-2019-11091, CVE-2019-3882, CVE-2019-9003, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1241-1

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-May/005460.html

SuSE SLED 12 SP4
x86_64
kernel-default-extra-4.12.14-95.16.1
kernel-default-4.12.14-95.16.1
kernel-syms-4.12.14-95.16.1
kernel-default-extra-debuginfo-4.12.14-95.16.1
kernel-default-devel-4.12.14-95.16.1
kernel-default-devel-debuginfo-4.12.14-95.16.1
kernel-default-debugsource-4.12.14-95.16.1
kernel-default-debuginfo-4.12.14-95.16.1

noarch
kernel-macros-4.12.14-95.16.1
kernel-devel-4.12.14-95.16.1
kernel-source-4.12.14-95.16.1

SuSE SLES 12 SP4
noarch
kernel-macros-4.12.14-95.16.1
kernel-devel-4.12.14-95.16.1
kernel-source-4.12.14-95.16.1

x86_64
kernel-default-base-debuginfo-4.12.14-95.16.1
kernel-default-base-4.12.14-95.16.1
kernel-default-4.12.14-95.16.1
kernel-syms-4.12.14-95.16.1

kernel-default-devel-4.12.14-95.16.1
kernel-default-devel-debuginfo-4.12.14-95.16.1
kernel-default-debugsource-4.12.14-95.16.1
kernel-default-debuginfo-4.12.14-95.16.1

147946 - SuSE Linux 15.0 openSUSE-SU-2019:1344-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5418, CVE-2019-5419

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1344-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00041.html

SuSE Linux 15.0
x86_64
ruby2.5-rubygem-actionpack-doc-5_1-5.1.4-lp150.2.3.1
ruby2.5-rubygem-actionpack-5_1-5.1.4-lp150.2.3.1

160556 - CentOS 7 CESA-2019-1017 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3839

Description

The scan detected that the host is missing the following update:
CESA-2019-1017

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-May/023301.html

CentOS 7
i686
ghostscript-devel-9.07-31.el7_6.11
ghostscript-9.07-31.el7_6.11

noarch
ghostscript-doc-9.07-31.el7_6.11

x86_64
ghostscript-gtk-9.07-31.el7_6.11
ghostscript-devel-9.07-31.el7_6.11
ghostscript-9.07-31.el7_6.11
ghostscript-cups-9.07-31.el7_6.11

163854 - Oracle Enterprise Linux ELSA-2019-1181 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-1181

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008728.html

OEL6
x86_64
qemu-kvm-0.12.1.2-2.506.el6_10.3
qemu-kvm-tools-0.12.1.2-2.506.el6_10.3
qemu-img-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3

i386
qemu-guest-agent-0.12.1.2-2.506.el6_10.3

163855 - Oracle Enterprise Linux ELSA-2019-1131 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11234, CVE-2019-11235

Description

The scan detected that the host is missing the following update:
ELSA-2019-1131

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008706.html

OEL7
x86_64
freeradius-ldap-3.0.13-10.el7_6
freeradius-postgresql-3.0.13-10.el7_6
freeradius-mysql-3.0.13-10.el7_6
freeradius-perl-3.0.13-10.el7_6
freeradius-sqlite-3.0.13-10.el7_6
freeradius-3.0.13-10.el7_6
freeradius-krb5-3.0.13-10.el7_6
freeradius-python-3.0.13-10.el7_6
freeradius-unixODBC-3.0.13-10.el7_6
freeradius-doc-3.0.13-10.el7_6
freeradius-devel-3.0.13-10.el7_6
freeradius-utils-3.0.13-10.el7_6

163856 - Oracle Enterprise Linux ELSA-2019-4629 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-4629

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008718.html
http://oss.oracle.com/pipermail/el-errata/2019-May/008717.html

OEL7
x86_64
kernel-uek-debug-4.1.12-124.26.12.el7uek
kernel-uek-devel-4.1.12-124.26.12.el7uek
kernel-uek-debug-devel-4.1.12-124.26.12.el7uek
kernel-uek-doc-4.1.12-124.26.12.el7uek
kernel-uek-firmware-4.1.12-124.26.12.el7uek
kernel-uek-4.1.12-124.26.12.el7uek

OEL6
x86_64
kernel-uek-4.1.12-124.26.12.el6uek
kernel-uek-firmware-4.1.12-124.26.12.el6uek
kernel-uek-devel-4.1.12-124.26.12.el6uek
kernel-uek-debug-devel-4.1.12-124.26.12.el6uek
kernel-uek-doc-4.1.12-124.26.12.el6uek
kernel-uek-debug-4.1.12-124.26.12.el6uek

163858 - Oracle Enterprise Linux ELSA-2019-4637 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-4637

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008725.html

OEL6
x86_64
kernel-uek-doc-2.6.39-400.310.1.el6uek
kernel-uek-devel-2.6.39-400.310.1.el6uek

kernel-uek-firmware-2.6.39-400.310.1.el6uek
kernel-uek-debug-devel-2.6.39-400.310.1.el6uek
kernel-uek-debug-2.6.39-400.310.1.el6uek
kernel-uek-2.6.39-400.310.1.el6uek

i386
kernel-uek-doc-2.6.39-400.310.1.el6uek
kernel-uek-devel-2.6.39-400.310.1.el6uek
kernel-uek-firmware-2.6.39-400.310.1.el6uek
kernel-uek-debug-devel-2.6.39-400.310.1.el6uek
kernel-uek-debug-2.6.39-400.310.1.el6uek
kernel-uek-2.6.39-400.310.1.el6uek

163860 - Oracle Enterprise Linux ELSA-2019-1180 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-1180

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008727.html

OEL6
x86_64
libvirt-python-0.10.2-64.0.1.el6_10.1
libvirt-lock-sanlock-0.10.2-64.0.1.el6_10.1
libvirt-client-0.10.2-64.0.1.el6_10.1
libvirt-0.10.2-64.0.1.el6_10.1
libvirt-devel-0.10.2-64.0.1.el6_10.1

i386
libvirt-python-0.10.2-64.0.1.el6_10.1
libvirt-client-0.10.2-64.0.1.el6_10.1
libvirt-0.10.2-64.0.1.el6_10.1
libvirt-devel-0.10.2-64.0.1.el6_10.1

163861 - Oracle Enterprise Linux ELSA-2019-1169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-1169

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008729.html

OEL6
x86_64
python-perf-2.6.32-754.14.2.el6
kernel-doc-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
kernel-abi-whitelists-2.6.32-754.14.2.el6
kernel-firmware-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

i386
python-perf-2.6.32-754.14.2.el6
kernel-doc-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
kernel-abi-whitelists-2.6.32-754.14.2.el6
kernel-firmware-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

163862 - Oracle Enterprise Linux ELSA-2019-4628 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-4628

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008716.html

OEL7
x86_64
kernel-uek-debug-devel-4.14.35-1844.4.5.2.el7uek
kernel-uek-doc-4.14.35-1844.4.5.2.el7uek
kernel-uek-debug-4.14.35-1844.4.5.2.el7uek
kernel-uek-devel-4.14.35-1844.4.5.2.el7uek
kernel-uek-tools-4.14.35-1844.4.5.2.el7uek
kernel-uek-4.14.35-1844.4.5.2.el7uek

163864 - Oracle Enterprise Linux ELSA-2019-4636 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ELSA-2019-4636

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008719.html
http://oss.oracle.com/pipermail/el-errata/2019-May/008720.html

OEL7
x86_64
kernel-uek-3.8.13-118.33.2.el7uek
dtrace-modules-3.8.13-118.33.2.el7uek-0.4.5-3.el7
kernel-uek-firmware-3.8.13-118.33.2.el7uek
kernel-uek-doc-3.8.13-118.33.2.el7uek
kernel-uek-debug-3.8.13-118.33.2.el7uek
kernel-uek-devel-3.8.13-118.33.2.el7uek
kernel-uek-debug-devel-3.8.13-118.33.2.el7uek

OEL6
x86_64
dtrace-modules-3.8.13-118.33.2.el6uek-0.4.5-3.el6
kernel-uek-doc-3.8.13-118.33.2.el6uek
kernel-uek-devel-3.8.13-118.33.2.el6uek
kernel-uek-firmware-3.8.13-118.33.2.el6uek
kernel-uek-debug-devel-3.8.13-118.33.2.el6uek
kernel-uek-3.8.13-118.33.2.el6uek
kernel-uek-debug-3.8.13-118.33.2.el6uek

171094 - Amazon Linux AMI ALAS-2019-1205 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
ALAS-2019-1205

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1205.html

Amazon Linux AMI
x86_64
kernel-tools-debuginfo-4.14.114-83.126.amzn1
kernel-devel-4.14.114-83.126.amzn1
kernel-tools-devel-4.14.114-83.126.amzn1
perf-4.14.114-83.126.amzn1
kernel-headers-4.14.114-83.126.amzn1
kernel-debuginfo-common-x86_64-4.14.114-83.126.amzn1

kernel-tools-4.14.114-83.126.amzn1
kernel-debuginfo-4.14.114-83.126.amzn1
perf-debuginfo-4.14.114-83.126.amzn1
kernel-4.14.114-83.126.amzn1

i686
kernel-debuginfo-common-i686-4.14.114-83.126.amzn1
kernel-devel-4.14.114-83.126.amzn1
kernel-tools-debuginfo-4.14.114-83.126.amzn1
kernel-tools-devel-4.14.114-83.126.amzn1
perf-4.14.114-83.126.amzn1
kernel-debuginfo-4.14.114-83.126.amzn1
kernel-headers-4.14.114-83.126.amzn1
kernel-tools-4.14.114-83.126.amzn1
perf-debuginfo-4.14.114-83.126.amzn1
kernel-4.14.114-83.126.amzn1

195152 - Fedora Linux 28 FEDORA-2019-f563e66380 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-2922, CVE-2018-7602, CVE-2019-11358

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f563e66380

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/2019/5/?count=200&page=3

Fedora Core 28

drupal7-7.66-1.fc28

195156 - Fedora Linux 28 FEDORA-2019-a4ed7400f4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a4ed7400f4

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/2019/5/?count=200&page=1

Fedora Core 28

httpd-2.4.39-1.1.fc28

195166 - Fedora Linux 30 FEDORA-2019-1cfe24db5c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5418, CVE-2019-5419, CVE-2019-5420

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1cfe24db5c

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/2019/5/?count=200&page=3

Fedora Core 30

rubygem-activerecord-5.2.3-1.fc30
rubygem-actioncable-5.2.3-1.fc30
rubygem-activesupport-5.2.3-1.fc30
rubygem-actionpack-5.2.3-2.fc30
rubygem-activestorage-5.2.3-1.fc30
rubygem-activejob-5.2.3-1.fc30
rubygem-railties-5.2.3-1.fc30
rubygem-actionmailer-5.2.3-1.fc30
rubygem-actionview-5.2.3-2.fc30
rubygem-activemodel-5.2.3-2.fc30
rubygem-rails-5.2.3-1.fc30

196308 - Red Hat Enterprise Linux RHSA-2019-1228 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
RHSA-2019-1228

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00044.html

RHEL7D
x86_64
wget-debuginfo-1.14-18.el7_6.1
wget-1.14-18.el7_6.1

RHEL7S
x86_64
wget-debuginfo-1.14-18.el7_6.1
wget-1.14-18.el7_6.1

RHEL7WS
x86_64
wget-debuginfo-1.14-18.el7_6.1
wget-1.14-18.el7_6.1

196309 - Red Hat Enterprise Linux RHSA-2019-1197 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1197

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00074.html

RHEL6_5S
x86_64
libvirt-lock-sanlock-0.10.2-29.el6_5.18
libvirt-debuginfo-0.10.2-29.el6_5.18
libvirt-devel-0.10.2-29.el6_5.18
libvirt-client-0.10.2-29.el6_5.18
libvirt-0.10.2-29.el6_5.18
libvirt-python-0.10.2-29.el6_5.18

196310 - Red Hat Enterprise Linux RHSA-2019-1177 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1177

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00055.html

RHEL7D
x86_64
libvirt-bash-completion-4.5.0-10.el7_6.9
libvirt-docs-4.5.0-10.el7_6.9
libvirt-daemon-lxc-4.5.0-10.el7_6.9
libvirt-daemon-config-nwfilter-4.5.0-10.el7_6.9
libvirt-nss-4.5.0-10.el7_6.9
libvirt-daemon-driver-secret-4.5.0-10.el7_6.9
libvirt-lock-sanlock-4.5.0-10.el7_6.9

libvirt-daemon-driver-interface-4.5.0-10.el7_6.9
libvirt-4.5.0-10.el7_6.9
libvirt-debuginfo-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-rbd-4.5.0-10.el7_6.9
libvirt-client-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-core-4.5.0-10.el7_6.9
libvirt-daemon-driver-network-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-gluster-4.5.0-10.el7_6.9
libvirt-devel-4.5.0-10.el7_6.9
libvirt-daemon-config-network-4.5.0-10.el7_6.9
libvirt-daemon-driver-qemu-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-disk-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-4.5.0-10.el7_6.9
libvirt-libs-4.5.0-10.el7_6.9
libvirt-admin-4.5.0-10.el7_6.9
libvirt-daemon-4.5.0-10.el7_6.9
libvirt-daemon-driver-nodedev-4.5.0-10.el7_6.9
libvirt-login-shell-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-logical-4.5.0-10.el7_6.9
libvirt-daemon-kvm-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-mpath-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-iscsi-4.5.0-10.el7_6.9
libvirt-daemon-driver-lxc-4.5.0-10.el7_6.9
libvirt-daemon-driver-nwfilter-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-scsi-4.5.0-10.el7_6.9

RHEL7S
x86_64
libvirt-bash-completion-4.5.0-10.el7_6.9
libvirt-docs-4.5.0-10.el7_6.9
libvirt-daemon-lxc-4.5.0-10.el7_6.9
libvirt-daemon-config-nwfilter-4.5.0-10.el7_6.9
libvirt-nss-4.5.0-10.el7_6.9
libvirt-daemon-driver-secret-4.5.0-10.el7_6.9
libvirt-lock-sanlock-4.5.0-10.el7_6.9
libvirt-daemon-driver-interface-4.5.0-10.el7_6.9
libvirt-4.5.0-10.el7_6.9
libvirt-debuginfo-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-rbd-4.5.0-10.el7_6.9
libvirt-client-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-core-4.5.0-10.el7_6.9
libvirt-daemon-driver-network-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-gluster-4.5.0-10.el7_6.9
libvirt-devel-4.5.0-10.el7_6.9
libvirt-daemon-config-network-4.5.0-10.el7_6.9
libvirt-daemon-driver-qemu-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-disk-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-4.5.0-10.el7_6.9
libvirt-libs-4.5.0-10.el7_6.9
libvirt-admin-4.5.0-10.el7_6.9
libvirt-daemon-4.5.0-10.el7_6.9
libvirt-daemon-driver-nodedev-4.5.0-10.el7_6.9
libvirt-login-shell-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-logical-4.5.0-10.el7_6.9
libvirt-daemon-kvm-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-mpath-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-iscsi-4.5.0-10.el7_6.9
libvirt-daemon-driver-lxc-4.5.0-10.el7_6.9
libvirt-daemon-driver-nwfilter-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-scsi-4.5.0-10.el7_6.9

RHEL7WS
x86_64
libvirt-bash-completion-4.5.0-10.el7_6.9
libvirt-docs-4.5.0-10.el7_6.9
libvirt-daemon-lxc-4.5.0-10.el7_6.9
libvirt-daemon-config-nwfilter-4.5.0-10.el7_6.9
libvirt-nss-4.5.0-10.el7_6.9
libvirt-daemon-driver-secret-4.5.0-10.el7_6.9
libvirt-lock-sanlock-4.5.0-10.el7_6.9
libvirt-daemon-driver-interface-4.5.0-10.el7_6.9
libvirt-4.5.0-10.el7_6.9
libvirt-debuginfo-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-rbd-4.5.0-10.el7_6.9
libvirt-client-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-core-4.5.0-10.el7_6.9
libvirt-daemon-driver-network-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-gluster-4.5.0-10.el7_6.9
libvirt-devel-4.5.0-10.el7_6.9
libvirt-daemon-config-network-4.5.0-10.el7_6.9
libvirt-daemon-driver-qemu-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-disk-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-4.5.0-10.el7_6.9
libvirt-libs-4.5.0-10.el7_6.9
libvirt-admin-4.5.0-10.el7_6.9
libvirt-daemon-4.5.0-10.el7_6.9
libvirt-daemon-driver-nodedev-4.5.0-10.el7_6.9
libvirt-login-shell-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-logical-4.5.0-10.el7_6.9
libvirt-daemon-kvm-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-mpath-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-iscsi-4.5.0-10.el7_6.9
libvirt-daemon-driver-lxc-4.5.0-10.el7_6.9
libvirt-daemon-driver-nwfilter-4.5.0-10.el7_6.9
libvirt-daemon-driver-storage-scsi-4.5.0-10.el7_6.9

196311 - Red Hat Enterprise Linux RHSA-2019-1147 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5418, CVE-2019-5419

Description

The scan detected that the host is missing the following update:
RHSA-2019-1147

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00028.html

RHEL6S
noarch
rh-ror50-rubygem-actionpack-doc-5.0.1-2.el6
rh-ror50-rubygem-actionpack-5.0.1-2.el6

RHEL6WS
noarch

rh-ror50-rubygem-actionpack-doc-5.0.1-2.el6
rh-ror50-rubygem-actionpack-5.0.1-2.el6

RHEL7S
noarch
rh-ror50-rubygem-actionpack-doc-5.0.1-2.el7
rh-ror50-rubygem-actionpack-5.0.1-2.el7

RHEL7WS
noarch
rh-ror50-rubygem-actionpack-doc-5.0.1-2.el7
rh-ror50-rubygem-actionpack-5.0.1-2.el7

196312 - Red Hat Enterprise Linux RHSA-2019-1193 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1193

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00063.html

RHEL6_6S
x86_64
python-perf-2.6.32-504.78.2.el6
kernel-headers-2.6.32-504.78.2.el6
kernel-debug-devel-2.6.32-504.78.2.el6
kernel-devel-2.6.32-504.78.2.el6
kernel-debuginfo-common-x86_64-2.6.32-504.78.2.el6
kernel-debug-2.6.32-504.78.2.el6
kernel-debuginfo-2.6.32-504.78.2.el6
perf-2.6.32-504.78.2.el6
kernel-2.6.32-504.78.2.el6
perf-debuginfo-2.6.32-504.78.2.el6
kernel-debug-debuginfo-2.6.32-504.78.2.el6
python-perf-debuginfo-2.6.32-504.78.2.el6

noarch
kernel-abi-whitelists-2.6.32-504.78.2.el6
kernel-doc-2.6.32-504.78.2.el6
kernel-firmware-2.6.32-504.78.2.el6

196314 - Red Hat Enterprise Linux RHSA-2019-1169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1169

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00049.html

RHEL6D
i386
python-perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-i686-2.6.32-754.14.2.el6
kernel-debug-debuginfo-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
python-perf-debuginfo-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
perf-debuginfo-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
kernel-debuginfo-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

noarch
kernel-doc-2.6.32-754.14.2.el6
kernel-abi-whitelists-2.6.32-754.14.2.el6
kernel-firmware-2.6.32-754.14.2.el6

x86_64
kernel-debug-debuginfo-2.6.32-754.14.2.el6
kernel-debuginfo-2.6.32-754.14.2.el6
python-perf-debuginfo-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-i686-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
perf-debuginfo-2.6.32-754.14.2.el6
python-perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-x86_64-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

RHEL6S
i386
python-perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-i686-2.6.32-754.14.2.el6
kernel-debug-debuginfo-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
python-perf-debuginfo-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
perf-debuginfo-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
kernel-debuginfo-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

noarch

kernel-doc-2.6.32-754.14.2.el6
kernel-abi-whitelists-2.6.32-754.14.2.el6
kernel-firmware-2.6.32-754.14.2.el6

x86_64
kernel-debug-debuginfo-2.6.32-754.14.2.el6
kernel-debuginfo-2.6.32-754.14.2.el6
python-perf-debuginfo-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-i686-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
perf-debuginfo-2.6.32-754.14.2.el6
python-perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-x86_64-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

RHEL6WS
i386
kernel-debuginfo-common-i686-2.6.32-754.14.2.el6
kernel-debug-debuginfo-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
python-perf-debuginfo-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
perf-debuginfo-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
kernel-debuginfo-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

noarch
kernel-doc-2.6.32-754.14.2.el6
kernel-abi-whitelists-2.6.32-754.14.2.el6
kernel-firmware-2.6.32-754.14.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-754.14.2.el6
kernel-debug-debuginfo-2.6.32-754.14.2.el6
kernel-debug-2.6.32-754.14.2.el6
python-perf-debuginfo-2.6.32-754.14.2.el6
perf-2.6.32-754.14.2.el6
kernel-debuginfo-common-x86_64-2.6.32-754.14.2.el6
kernel-debug-devel-2.6.32-754.14.2.el6
perf-debuginfo-2.6.32-754.14.2.el6
kernel-devel-2.6.32-754.14.2.el6
kernel-debuginfo-2.6.32-754.14.2.el6
kernel-2.6.32-754.14.2.el6
kernel-headers-2.6.32-754.14.2.el6

196315 - Red Hat Enterprise Linux RHSA-2019-1149 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5418, CVE-2019-5419

Description

The scan detected that the host is missing the following update:
RHSA-2019-1149

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00030.html

RHEL6S
noarch
rh-ror42-rubygem-actionpack-4.2.6-5.el6
rh-ror42-rubygem-actionpack-doc-4.2.6-5.el6

RHEL6WS
noarch
rh-ror42-rubygem-actionpack-4.2.6-5.el6
rh-ror42-rubygem-actionpack-doc-4.2.6-5.el6

RHEL7S
noarch
rh-ror42-rubygem-actionpack-doc-4.2.6-5.el7
rh-ror42-rubygem-actionpack-4.2.6-5.el7

RHEL7WS
noarch
rh-ror42-rubygem-actionpack-doc-4.2.6-5.el7
rh-ror42-rubygem-actionpack-4.2.6-5.el7

196316 - Red Hat Enterprise Linux RHSA-2019-1195 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1195

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00062.html

RHEL6_6S
x86_64
qemu-kvm-0.12.1.2-2.448.el6_6.8
qemu-img-0.12.1.2-2.448.el6_6.8
qemu-kvm-debuginfo-0.12.1.2-2.448.el6_6.8
qemu-guest-agent-0.12.1.2-2.448.el6_6.8
qemu-kvm-tools-0.12.1.2-2.448.el6_6.8

196318 - Red Hat Enterprise Linux RHSA-2019-1181 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1181

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00048.html

RHEL6D
x86_64
qemu-kvm-0.12.1.2-2.506.el6_10.3
qemu-kvm-tools-0.12.1.2-2.506.el6_10.3
qemu-img-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3
qemu-kvm-debuginfo-0.12.1.2-2.506.el6_10.3

i386
qemu-kvm-debuginfo-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3

RHEL6S
i386
qemu-kvm-debuginfo-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3

x86_64
qemu-kvm-0.12.1.2-2.506.el6_10.3
qemu-kvm-tools-0.12.1.2-2.506.el6_10.3
qemu-img-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3
qemu-kvm-debuginfo-0.12.1.2-2.506.el6_10.3

RHEL6WS
x86_64
qemu-kvm-0.12.1.2-2.506.el6_10.3
qemu-kvm-tools-0.12.1.2-2.506.el6_10.3
qemu-img-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3
qemu-kvm-debuginfo-0.12.1.2-2.506.el6_10.3

i386
qemu-kvm-debuginfo-0.12.1.2-2.506.el6_10.3
qemu-guest-agent-0.12.1.2-2.506.el6_10.3

196319 - Red Hat Enterprise Linux RHSA-2019-1151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8324

Description

The scan detected that the host is missing the following update:
RHSA-2019-1151

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00032.html

RHEL6S
x86_64
rh-ruby23-ruby-devel-2.3.8-70.el6
rh-ruby23-rubygem-psych-2.1.0.1-70.el6
rh-ruby23-rubygem-bigdecimal-1.2.8-70.el6
rh-ruby23-rubygem-did_you_mean-1.0.0-70.el6
rh-ruby23-ruby-2.3.8-70.el6
rh-ruby23-rubygem-net-telnet-0.1.1-70.el6
rh-ruby23-rubygem-io-console-0.4.5-70.el6
rh-ruby23-ruby-tcltk-2.3.8-70.el6
rh-ruby23-ruby-libs-2.3.8-70.el6
rh-ruby23-ruby-debuginfo-2.3.8-70.el6
rh-ruby23-rubygem-json-1.8.3.1-70.el6

noarch
rh-ruby23-ruby-irb-2.3.8-70.el6
rh-ruby23-rubygem-rdoc-4.2.1-70.el6
rh-ruby23-rubygem-rake-10.4.2-70.el6
rh-ruby23-rubygem-minitest-5.8.5-70.el6
rh-ruby23-rubygem-test-unit-3.1.5-70.el6
rh-ruby23-ruby-doc-2.3.8-70.el6
rh-ruby23-rubygems-devel-2.5.2.3-70.el6
rh-ruby23-rubygems-2.5.2.3-70.el6
rh-ruby23-rubygem-power_assert-0.2.6-70.el6

RHEL6WS
x86_64
rh-ruby23-ruby-devel-2.3.8-70.el6
rh-ruby23-rubygem-psych-2.1.0.1-70.el6
rh-ruby23-rubygem-bigdecimal-1.2.8-70.el6
rh-ruby23-rubygem-did_you_mean-1.0.0-70.el6
rh-ruby23-ruby-2.3.8-70.el6
rh-ruby23-rubygem-net-telnet-0.1.1-70.el6
rh-ruby23-rubygem-io-console-0.4.5-70.el6
rh-ruby23-ruby-tcltk-2.3.8-70.el6
rh-ruby23-ruby-libs-2.3.8-70.el6
rh-ruby23-ruby-debuginfo-2.3.8-70.el6
rh-ruby23-rubygem-json-1.8.3.1-70.el6

noarch
rh-ruby23-ruby-irb-2.3.8-70.el6
rh-ruby23-rubygem-rdoc-4.2.1-70.el6
rh-ruby23-rubygem-rake-10.4.2-70.el6
rh-ruby23-rubygem-minitest-5.8.5-70.el6
rh-ruby23-rubygem-test-unit-3.1.5-70.el6
rh-ruby23-ruby-doc-2.3.8-70.el6
rh-ruby23-rubygems-devel-2.5.2.3-70.el6
rh-ruby23-rubygems-2.5.2.3-70.el6
rh-ruby23-rubygem-power_assert-0.2.6-70.el6

RHEL7S
x86_64
rh-ruby23-rubygem-json-1.8.3.1-70.el7

rh-ruby23-ruby-libs-2.3.8-70.el7
rh-ruby23-ruby-devel-2.3.8-70.el7
rh-ruby23-rubygem-did_you_mean-1.0.0-70.el7
rh-ruby23-ruby-2.3.8-70.el7
rh-ruby23-rubygem-net-telnet-0.1.1-70.el7
rh-ruby23-rubygem-io-console-0.4.5-70.el7
rh-ruby23-rubygem-psych-2.1.0.1-70.el7
rh-ruby23-ruby-tcltk-2.3.8-70.el7
rh-ruby23-rubygem-bigdecimal-1.2.8-70.el7
rh-ruby23-ruby-debuginfo-2.3.8-70.el7

noarch
rh-ruby23-rubygem-test-unit-3.1.5-70.el7
rh-ruby23-ruby-irb-2.3.8-70.el7
rh-ruby23-rubygem-rdoc-4.2.1-70.el7
rh-ruby23-rubygem-minitest-5.8.5-70.el7
rh-ruby23-ruby-doc-2.3.8-70.el7
rh-ruby23-rubygem-rake-10.4.2-70.el7
rh-ruby23-rubygems-2.5.2.3-70.el7
rh-ruby23-rubygems-devel-2.5.2.3-70.el7
rh-ruby23-rubygem-power_assert-0.2.6-70.el7

RHEL7WS
x86_64
rh-ruby23-rubygem-json-1.8.3.1-70.el7
rh-ruby23-ruby-libs-2.3.8-70.el7
rh-ruby23-ruby-devel-2.3.8-70.el7
rh-ruby23-rubygem-did_you_mean-1.0.0-70.el7
rh-ruby23-ruby-2.3.8-70.el7
rh-ruby23-rubygem-net-telnet-0.1.1-70.el7
rh-ruby23-rubygem-io-console-0.4.5-70.el7
rh-ruby23-rubygem-psych-2.1.0.1-70.el7
rh-ruby23-ruby-tcltk-2.3.8-70.el7
rh-ruby23-rubygem-bigdecimal-1.2.8-70.el7
rh-ruby23-ruby-debuginfo-2.3.8-70.el7

noarch
rh-ruby23-rubygem-test-unit-3.1.5-70.el7
rh-ruby23-ruby-irb-2.3.8-70.el7
rh-ruby23-rubygem-rdoc-4.2.1-70.el7
rh-ruby23-rubygem-minitest-5.8.5-70.el7
rh-ruby23-ruby-doc-2.3.8-70.el7
rh-ruby23-rubygem-rake-10.4.2-70.el7
rh-ruby23-rubygems-2.5.2.3-70.el7
rh-ruby23-rubygems-devel-2.5.2.3-70.el7
rh-ruby23-rubygem-power_assert-0.2.6-70.el7

196320 - Red Hat Enterprise Linux RHSA-2019-1131 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11234, CVE-2019-11235

Description

The scan detected that the host is missing the following update:
RHSA-2019-1131

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00021.html

RHEL7S
x86_64
freeradius-3.0.13-10.el7_6
freeradius-krb5-3.0.13-10.el7_6
freeradius-perl-3.0.13-10.el7_6
freeradius-utils-3.0.13-10.el7_6
freeradius-sqlite-3.0.13-10.el7_6
freeradius-unixODBC-3.0.13-10.el7_6
freeradius-postgresql-3.0.13-10.el7_6
freeradius-doc-3.0.13-10.el7_6
freeradius-debuginfo-3.0.13-10.el7_6
freeradius-ldap-3.0.13-10.el7_6
freeradius-mysql-3.0.13-10.el7_6
freeradius-python-3.0.13-10.el7_6
freeradius-devel-3.0.13-10.el7_6

RHEL7WS
x86_64
freeradius-3.0.13-10.el7_6
freeradius-krb5-3.0.13-10.el7_6
freeradius-perl-3.0.13-10.el7_6
freeradius-utils-3.0.13-10.el7_6
freeradius-sqlite-3.0.13-10.el7_6
freeradius-unixODBC-3.0.13-10.el7_6
freeradius-postgresql-3.0.13-10.el7_6
freeradius-doc-3.0.13-10.el7_6
freeradius-debuginfo-3.0.13-10.el7_6
freeradius-ldap-3.0.13-10.el7_6
freeradius-mysql-3.0.13-10.el7_6
freeradius-python-3.0.13-10.el7_6
freeradius-devel-3.0.13-10.el7_6

196321 - Red Hat Enterprise Linux RHSA-2019-1198 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1198

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00065.html

RHEL6_5S
x86_64
qemu-img-0.12.1.2-2.415.el6_5.20
qemu-guest-agent-0.12.1.2-2.415.el6_5.20
qemu-kvm-tools-0.12.1.2-2.415.el6_5.20

qemu-kvm-0.12.1.2-2.415.el6_5.20
qemu-kvm-debuginfo-0.12.1.2-2.415.el6_5.20

196322 - Red Hat Enterprise Linux RHSA-2019-1168 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1168

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00054.html

RHEL7D
x86_64
bpftool-3.10.0-957.12.2.el7
perf-3.10.0-957.12.2.el7
kernel-devel-3.10.0-957.12.2.el7
perf-debuginfo-3.10.0-957.12.2.el7
kernel-3.10.0-957.12.2.el7
kernel-debug-devel-3.10.0-957.12.2.el7
python-perf-3.10.0-957.12.2.el7
kernel-debuginfo-3.10.0-957.12.2.el7
kernel-tools-libs-devel-3.10.0-957.12.2.el7
kernel-tools-debuginfo-3.10.0-957.12.2.el7
python-perf-debuginfo-3.10.0-957.12.2.el7
kernel-debug-3.10.0-957.12.2.el7
kernel-debuginfo-common-x86_64-3.10.0-957.12.2.el7
kernel-headers-3.10.0-957.12.2.el7
kernel-tools-3.10.0-957.12.2.el7
kernel-tools-libs-3.10.0-957.12.2.el7
kernel-debug-debuginfo-3.10.0-957.12.2.el7

noarch
kernel-doc-3.10.0-957.12.2.el7
kernel-abi-whitelists-3.10.0-957.12.2.el7

RHEL7S
noarch
kernel-doc-3.10.0-957.12.2.el7
kernel-abi-whitelists-3.10.0-957.12.2.el7

x86_64
bpftool-3.10.0-957.12.2.el7
perf-3.10.0-957.12.2.el7
kernel-devel-3.10.0-957.12.2.el7
perf-debuginfo-3.10.0-957.12.2.el7
kernel-3.10.0-957.12.2.el7
kernel-debug-devel-3.10.0-957.12.2.el7
python-perf-3.10.0-957.12.2.el7
kernel-debuginfo-3.10.0-957.12.2.el7
kernel-tools-libs-devel-3.10.0-957.12.2.el7

kernel-tools-debuginfo-3.10.0-957.12.2.el7
python-perf-debuginfo-3.10.0-957.12.2.el7
kernel-debug-3.10.0-957.12.2.el7
kernel-debuginfo-common-x86_64-3.10.0-957.12.2.el7
kernel-headers-3.10.0-957.12.2.el7
kernel-tools-3.10.0-957.12.2.el7
kernel-tools-libs-3.10.0-957.12.2.el7
kernel-debug-debuginfo-3.10.0-957.12.2.el7

RHEL7WS
x86_64
bpftool-3.10.0-957.12.2.el7
perf-3.10.0-957.12.2.el7
kernel-devel-3.10.0-957.12.2.el7
perf-debuginfo-3.10.0-957.12.2.el7
kernel-3.10.0-957.12.2.el7
kernel-debug-devel-3.10.0-957.12.2.el7
python-perf-3.10.0-957.12.2.el7
kernel-debuginfo-3.10.0-957.12.2.el7
kernel-tools-libs-devel-3.10.0-957.12.2.el7
kernel-tools-debuginfo-3.10.0-957.12.2.el7
python-perf-debuginfo-3.10.0-957.12.2.el7
kernel-debug-3.10.0-957.12.2.el7
kernel-debuginfo-common-x86_64-3.10.0-957.12.2.el7
kernel-headers-3.10.0-957.12.2.el7
kernel-tools-3.10.0-957.12.2.el7
kernel-tools-libs-3.10.0-957.12.2.el7
kernel-debug-debuginfo-3.10.0-957.12.2.el7

noarch
kernel-doc-3.10.0-957.12.2.el7
kernel-abi-whitelists-3.10.0-957.12.2.el7

196323 - Red Hat Enterprise Linux RHSA-2019-1178 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1178

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00057.html

RHEL7D
x86_64
qemu-img-1.5.3-160.el7_6.2
qemu-kvm-tools-1.5.3-160.el7_6.2
qemu-kvm-1.5.3-160.el7_6.2
qemu-kvm-common-1.5.3-160.el7_6.2
qemu-kvm-debuginfo-1.5.3-160.el7_6.2

RHEL7S

x86_64
qemu-img-1.5.3-160.el7_6.2
qemu-kvm-tools-1.5.3-160.el7_6.2
qemu-kvm-1.5.3-160.el7_6.2
qemu-kvm-common-1.5.3-160.el7_6.2
qemu-kvm-debuginfo-1.5.3-160.el7_6.2

RHEL7WS
x86_64
qemu-img-1.5.3-160.el7_6.2
qemu-kvm-tools-1.5.3-160.el7_6.2
qemu-kvm-1.5.3-160.el7_6.2
qemu-kvm-common-1.5.3-160.el7_6.2
qemu-kvm-debuginfo-1.5.3-160.el7_6.2

196324 - Red Hat Enterprise Linux RHSA-2019-1148 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Description

The scan detected that the host is missing the following update:
RHSA-2019-1148

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00029.html

RHEL7S
noarch
rh-ruby25-rubygems-devel-2.7.6.2-7.el7
rh-ruby25-ruby-doc-2.5.5-7.el7
rh-ruby25-ruby-irb-2.5.5-7.el7
rh-ruby25-rubygem-power_assert-1.1.1-7.el7
rh-ruby25-rubygem-rdoc-6.0.1-7.el7
rh-ruby25-rubygem-did_you_mean-1.2.0-7.el7
rh-ruby25-rubygem-xmlrpc-0.3.0-7.el7
rh-ruby25-rubygems-2.7.6.2-7.el7
rh-ruby25-rubygem-net-telnet-0.1.1-7.el7
rh-ruby25-rubygem-test-unit-3.2.7-7.el7
rh-ruby25-rubygem-rake-12.3.0-7.el7
rh-ruby25-rubygem-minitest-5.10.3-7.el7

RHEL7WS
x86_64
rh-ruby25-rubygem-psych-3.0.2-7.el7
rh-ruby25-rubygem-openssl-2.1.2-7.el7
rh-ruby25-rubygem-bigdecimal-1.3.4-7.el7
rh-ruby25-ruby-debuginfo-2.5.5-7.el7
rh-ruby25-rubygem-json-2.1.0-7.el7
rh-ruby25-ruby-devel-2.5.5-7.el7
rh-ruby25-ruby-libs-2.5.5-7.el7
rh-ruby25-rubygem-io-console-0.4.6-7.el7
rh-ruby25-ruby-2.5.5-7.el7

noarch
rh-ruby25-rubygems-devel-2.7.6.2-7.el7
rh-ruby25-ruby-doc-2.5.5-7.el7
rh-ruby25-ruby-irb-2.5.5-7.el7
rh-ruby25-rubygem-power_assert-1.1.1-7.el7
rh-ruby25-rubygem-rdoc-6.0.1-7.el7
rh-ruby25-rubygem-did_you_mean-1.2.0-7.el7
rh-ruby25-rubygem-xmlrpc-0.3.0-7.el7
rh-ruby25-rubygems-2.7.6.2-7.el7
rh-ruby25-rubygem-net-telnet-0.1.1-7.el7
rh-ruby25-rubygem-test-unit-3.2.7-7.el7
rh-ruby25-rubygem-rake-12.3.0-7.el7
rh-ruby25-rubygem-minitest-5.10.3-7.el7

196325 - Red Hat Enterprise Linux RHSA-2019-1194 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1194

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00068.html

RHEL6_6S
x86_64
libvirt-0.10.2-46.el6_6.10
libvirt-client-0.10.2-46.el6_6.10
libvirt-debuginfo-0.10.2-46.el6_6.10
libvirt-python-0.10.2-46.el6_6.10
libvirt-devel-0.10.2-46.el6_6.10
libvirt-lock-sanlock-0.10.2-46.el6_6.10

196327 - Red Hat Enterprise Linux RHSA-2019-1180 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1180

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00050.html

RHEL6D

x86_64
libvirt-devel-0.10.2-64.el6_10.1
libvirt-client-0.10.2-64.el6_10.1
libvirt-lock-sanlock-0.10.2-64.el6_10.1
libvirt-python-0.10.2-64.el6_10.1
libvirt-0.10.2-64.el6_10.1
libvirt-debuginfo-0.10.2-64.el6_10.1

i386
libvirt-python-0.10.2-64.el6_10.1
libvirt-0.10.2-64.el6_10.1
libvirt-client-0.10.2-64.el6_10.1
libvirt-debuginfo-0.10.2-64.el6_10.1
libvirt-devel-0.10.2-64.el6_10.1

RHEL6S
i386
libvirt-devel-0.10.2-64.el6_10.1
libvirt-0.10.2-64.el6_10.1
libvirt-client-0.10.2-64.el6_10.1
libvirt-debuginfo-0.10.2-64.el6_10.1
libvirt-python-0.10.2-64.el6_10.1

x86_64
libvirt-client-0.10.2-64.el6_10.1
libvirt-python-0.10.2-64.el6_10.1
libvirt-lock-sanlock-0.10.2-64.el6_10.1
libvirt-0.10.2-64.el6_10.1
libvirt-devel-0.10.2-64.el6_10.1
libvirt-debuginfo-0.10.2-64.el6_10.1

RHEL6WS
x86_64
libvirt-devel-0.10.2-64.el6_10.1
libvirt-0.10.2-64.el6_10.1
libvirt-client-0.10.2-64.el6_10.1
libvirt-debuginfo-0.10.2-64.el6_10.1
libvirt-python-0.10.2-64.el6_10.1

i386
libvirt-devel-0.10.2-64.el6_10.1
libvirt-0.10.2-64.el6_10.1
libvirt-client-0.10.2-64.el6_10.1
libvirt-debuginfo-0.10.2-64.el6_10.1
libvirt-python-0.10.2-64.el6_10.1

196328 - Red Hat Enterprise Linux RHSA-2019-1150 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Description

The scan detected that the host is missing the following update:
RHSA-2019-1150

Observation

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

For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00031.html

RHEL6S
x86_64
rh-ruby24-rubygem-psych-2.2.2-92.el6
rh-ruby24-rubygem-openssl-2.0.9-92.el6
rh-ruby24-ruby-libs-2.4.6-92.el6
rh-ruby24-rubygem-did_you_mean-1.1.0-92.el6
rh-ruby24-rubygem-bigdecimal-1.3.2-92.el6
rh-ruby24-rubygem-net-telnet-0.1.1-92.el6
rh-ruby24-rubygem-io-console-0.4.6-92.el6
rh-ruby24-rubygem-json-2.0.4-92.el6
rh-ruby24-ruby-debuginfo-2.4.6-92.el6
rh-ruby24-ruby-devel-2.4.6-92.el6
rh-ruby24-ruby-2.4.6-92.el6

noarch
rh-ruby24-rubygems-devel-2.6.14.4-92.el6
rh-ruby24-rubygem-power_assert-0.4.1-92.el6
rh-ruby24-ruby-doc-2.4.6-92.el6
rh-ruby24-rubygem-rake-12.0.0-92.el6
rh-ruby24-rubygem-test-unit-3.2.3-92.el6
rh-ruby24-rubygem-minitest-5.10.1-92.el6
rh-ruby24-rubygem-xmlrpc-0.2.1-92.el6
rh-ruby24-ruby-irb-2.4.6-92.el6
rh-ruby24-rubygems-2.6.14.4-92.el6
rh-ruby24-rubygem-rdoc-5.0.0-92.el6

RHEL6WS
x86_64
rh-ruby24-rubygem-psych-2.2.2-92.el6
rh-ruby24-rubygem-openssl-2.0.9-92.el6
rh-ruby24-ruby-libs-2.4.6-92.el6
rh-ruby24-rubygem-did_you_mean-1.1.0-92.el6
rh-ruby24-rubygem-bigdecimal-1.3.2-92.el6
rh-ruby24-rubygem-net-telnet-0.1.1-92.el6
rh-ruby24-rubygem-io-console-0.4.6-92.el6
rh-ruby24-rubygem-json-2.0.4-92.el6
rh-ruby24-ruby-debuginfo-2.4.6-92.el6
rh-ruby24-ruby-devel-2.4.6-92.el6
rh-ruby24-ruby-2.4.6-92.el6

noarch
rh-ruby24-rubygems-devel-2.6.14.4-92.el6
rh-ruby24-rubygem-power_assert-0.4.1-92.el6
rh-ruby24-ruby-doc-2.4.6-92.el6
rh-ruby24-rubygem-rake-12.0.0-92.el6
rh-ruby24-rubygem-test-unit-3.2.3-92.el6
rh-ruby24-rubygem-minitest-5.10.1-92.el6
rh-ruby24-rubygem-xmlrpc-0.2.1-92.el6
rh-ruby24-ruby-irb-2.4.6-92.el6
rh-ruby24-rubygems-2.6.14.4-92.el6
rh-ruby24-rubygem-rdoc-5.0.0-92.el6

RHEL7S
x86_64
rh-ruby24-ruby-libs-2.4.6-92.el7
rh-ruby24-ruby-devel-2.4.6-92.el7

rh-ruby24-rubygem-did_you_mean-1.1.0-92.el7
rh-ruby24-rubygem-bigdecimal-1.3.2-92.el7
rh-ruby24-rubygem-json-2.0.4-92.el7
rh-ruby24-rubygem-io-console-0.4.6-92.el7
rh-ruby24-rubygem-net-telnet-0.1.1-92.el7
rh-ruby24-rubygem-openssl-2.0.9-92.el7
rh-ruby24-rubygem-psych-2.2.2-92.el7
rh-ruby24-ruby-debuginfo-2.4.6-92.el7
rh-ruby24-ruby-2.4.6-92.el7

noarch
rh-ruby24-rubygem-xmlrpc-0.2.1-92.el7
rh-ruby24-rubygem-minitest-5.10.1-92.el7
rh-ruby24-rubygems-devel-2.6.14.4-92.el7
rh-ruby24-rubygem-power_assert-0.4.1-92.el7
rh-ruby24-rubygem-rake-12.0.0-92.el7
rh-ruby24-ruby-doc-2.4.6-92.el7
rh-ruby24-rubygem-test-unit-3.2.3-92.el7
rh-ruby24-ruby-irb-2.4.6-92.el7
rh-ruby24-rubygem-rdoc-5.0.0-92.el7
rh-ruby24-rubygems-2.6.14.4-92.el7

RHEL7WS
x86_64
rh-ruby24-ruby-libs-2.4.6-92.el7
rh-ruby24-ruby-devel-2.4.6-92.el7
rh-ruby24-rubygem-did_you_mean-1.1.0-92.el7
rh-ruby24-rubygem-bigdecimal-1.3.2-92.el7
rh-ruby24-rubygem-json-2.0.4-92.el7
rh-ruby24-rubygem-io-console-0.4.6-92.el7
rh-ruby24-rubygem-net-telnet-0.1.1-92.el7
rh-ruby24-rubygem-openssl-2.0.9-92.el7
rh-ruby24-rubygem-psych-2.2.2-92.el7
rh-ruby24-ruby-debuginfo-2.4.6-92.el7
rh-ruby24-ruby-2.4.6-92.el7

noarch
rh-ruby24-rubygem-xmlrpc-0.2.1-92.el7
rh-ruby24-rubygem-minitest-5.10.1-92.el7
rh-ruby24-rubygems-devel-2.6.14.4-92.el7
rh-ruby24-rubygem-power_assert-0.4.1-92.el7
rh-ruby24-rubygem-rake-12.0.0-92.el7
rh-ruby24-ruby-doc-2.4.6-92.el7
rh-ruby24-rubygem-test-unit-3.2.3-92.el7
rh-ruby24-ruby-irb-2.4.6-92.el7
rh-ruby24-rubygem-rdoc-5.0.0-92.el7
rh-ruby24-rubygems-2.6.14.4-92.el7

196329 - Red Hat Enterprise Linux RHSA-2019-1196 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
RHSA-2019-1196

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00064.html

RHEL6_5S
x86_64
python-perf-2.6.32-431.94.2.el6
kernel-debug-2.6.32-431.94.2.el6
kernel-2.6.32-431.94.2.el6
kernel-devel-2.6.32-431.94.2.el6
kernel-debuginfo-common-x86_64-2.6.32-431.94.2.el6
perf-debuginfo-2.6.32-431.94.2.el6
perf-2.6.32-431.94.2.el6
python-perf-debuginfo-2.6.32-431.94.2.el6
kernel-debug-devel-2.6.32-431.94.2.el6
kernel-debug-debuginfo-2.6.32-431.94.2.el6
kernel-headers-2.6.32-431.94.2.el6
kernel-debuginfo-2.6.32-431.94.2.el6

noarch
kernel-firmware-2.6.32-431.94.2.el6
kernel-abi-whitelists-2.6.32-431.94.2.el6
kernel-doc-2.6.32-431.94.2.el6

25007 - (MSPT-May2019) Microsoft Azure DevOps Server and Team Foundation Server Cross-site Scripting (CVE-2019-0872)

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

Risk Level: Medium

CVE: CVE-2019-0872

Description

A vulnerability in some versions of Microsoft Azure DevOps Server and Team Foundation Server could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to remote code execution.

The flaw is due to improper handling of user inputs. Successful exploitation by an authenticated attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25111 - (MSPT-May2019) Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-0933)

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

Risk Level: Medium

CVE: CVE-2019-0933

Description

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

Observation

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

The flaw lies in the chakra scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25112 - (MSPT-May2019) Microsoft Edge Chakra Scripting Engine Memory Corruption Vulnerability (CVE-2019-0937)

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

Risk Level: Medium

CVE: CVE-2019-0937

Description

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

Observation

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

The flaw lies in the chakra scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25139 - (MSPT-May2019) Microsoft SharePoint Server Cross-site Scripting (CVE-2019-0963)

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

Risk Level: Medium

CVE: CVE-2019-0963

Description

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

Observation

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

The flaw is due to improper handling of a specially crafted web request. Successful exploitation by an authenticated attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

147920 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1219-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2018-3639, CVE-2019-2422, CVE-2019-2426, CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1219-1

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-May/005446.html

SuSE SLED 12 SP3
x86_64

java-1_8_0-openjdk-headless-1.8.0.212-27.32.1
java-1_8_0-openjdk-1.8.0.212-27.32.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debugsource-1.8.0.212-27.32.1

SuSE SLED 12 SP4
x86_64
java-1_8_0-openjdk-headless-1.8.0.212-27.32.1
java-1_8_0-openjdk-1.8.0.212-27.32.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debugsource-1.8.0.212-27.32.1

SuSE SLES 12 SP4
x86_64
java-1_8_0-openjdk-headless-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debugsource-1.8.0.212-27.32.1
java-1_8_0-openjdk-devel-1.8.0.212-27.32.1
java-1_8_0-openjdk-1.8.0.212-27.32.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-headless-1.8.0.212-27.32.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-demo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debuginfo-1.8.0.212-27.32.1

SuSE SLES 12 SP3
x86_64
java-1_8_0-openjdk-headless-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debugsource-1.8.0.212-27.32.1
java-1_8_0-openjdk-devel-1.8.0.212-27.32.1
java-1_8_0-openjdk-1.8.0.212-27.32.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-headless-1.8.0.212-27.32.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.212-27.32.1
java-1_8_0-openjdk-demo-1.8.0.212-27.32.1
java-1_8_0-openjdk-debuginfo-1.8.0.212-27.32.1

147929 - SuSE Linux 42.3 openSUSE-SU-2019:1355-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11008, CVE-2019-11009, CVE-2019-11473, CVE-2019-11474, CVE-2019-11505, CVE-2019-11506

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1355-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00055.html

SuSE Linux 42.3
x86_64
GraphicsMagick-debugsource-1.3.25-135.1
GraphicsMagick-1.3.25-135.1

libGraphicsMagick++-Q16-12-1.3.25-135.1
GraphicsMagick-debuginfo-1.3.25-135.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-135.1
libGraphicsMagick-Q16-3-1.3.25-135.1
perl-GraphicsMagick-debuginfo-1.3.25-135.1
libGraphicsMagickWand-Q16-2-1.3.25-135.1
libGraphicsMagick3-config-1.3.25-135.1
libGraphicsMagick++-devel-1.3.25-135.1
perl-GraphicsMagick-1.3.25-135.1
GraphicsMagick-devel-1.3.25-135.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-135.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-135.1

i586
GraphicsMagick-debugsource-1.3.25-135.1
GraphicsMagick-1.3.25-135.1
libGraphicsMagick++-Q16-12-1.3.25-135.1
GraphicsMagick-debuginfo-1.3.25-135.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-135.1
libGraphicsMagick-Q16-3-1.3.25-135.1
perl-GraphicsMagick-debuginfo-1.3.25-135.1
libGraphicsMagickWand-Q16-2-1.3.25-135.1
libGraphicsMagick3-config-1.3.25-135.1
libGraphicsMagick++-devel-1.3.25-135.1
perl-GraphicsMagick-1.3.25-135.1
GraphicsMagick-devel-1.3.25-135.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-135.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-135.1

147930 - SuSE Linux 15.0 openSUSE-SU-2019:1354-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11008, CVE-2019-11009, CVE-2019-11473, CVE-2019-11474, CVE-2019-11505, CVE-2019-11506

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1354-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00054.html

SuSE Linux 15.0
x86_64
libGraphicsMagick++-Q16-12-debuginfo-1.3.29-lp150.3.28.1
perl-GraphicsMagick-debuginfo-1.3.29-lp150.3.28.1
libGraphicsMagick-Q16-3-1.3.29-lp150.3.28.1
perl-GraphicsMagick-1.3.29-lp150.3.28.1
libGraphicsMagick++-Q16-12-1.3.29-lp150.3.28.1
GraphicsMagick-1.3.29-lp150.3.28.1
libGraphicsMagick++-devel-1.3.29-lp150.3.28.1
libGraphicsMagickWand-Q16-2-1.3.29-lp150.3.28.1
libGraphicsMagick3-config-1.3.29-lp150.3.28.1
libGraphicsMagick-Q16-3-debuginfo-1.3.29-lp150.3.28.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.29-lp150.3.28.1

GraphicsMagick-devel-1.3.29-lp150.3.28.1
GraphicsMagick-debugsource-1.3.29-lp150.3.28.1
GraphicsMagick-debuginfo-1.3.29-lp150.3.28.1

147935 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:1245-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000204, CVE-2018-10853, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-15594, CVE-2018-5814, CVE-2019-11091, CVE-2019-3882, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1245-1

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-May/005462.html
http://lists.suse.com/pipermail/sle-security-updates/2019-May/005456.html

SuSE SLED 12 SP3
x86_64
kernel-default-4.4.178-94.91.2
kernel-default-extra-4.4.178-94.91.2
kernel-default-debugsource-4.4.178-94.91.2
kernel-default-devel-4.4.178-94.91.2
kernel-default-debuginfo-4.4.178-94.91.2
kernel-default-extra-debuginfo-4.4.178-94.91.2
kernel-syms-4.4.178-94.91.1

noarch
kernel-macros-4.4.178-94.91.1
kernel-source-4.4.178-94.91.1
kernel-devel-4.4.178-94.91.1

SuSE SLES 12 SP3
noarch
kernel-macros-4.4.178-94.91.1
kernel-source-4.4.178-94.91.1
kernel-devel-4.4.178-94.91.1

x86_64
kernel-default-4.4.178-94.91.2
kernel-default-debugsource-4.4.178-94.91.2
kernel-default-devel-4.4.178-94.91.2
kernel-default-base-debuginfo-4.4.178-94.91.2
kernel-default-debuginfo-4.4.178-94.91.2
kernel-syms-4.4.178-94.91.1
kernel-default-base-4.4.178-94.91.2

160558 - CentOS 7 CESA-2019-1024 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10063

Description

The scan detected that the host is missing the following update:
CESA-2019-1024

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-May/023300.html

CentOS 7
x86_64
flatpak-1.0.2-5.el7_6
flatpak-devel-1.0.2-5.el7_6
flatpak-builder-1.0.0-5.el7_6
flatpak-libs-1.0.2-5.el7_6

163857 - Oracle Enterprise Linux ELSA-2019-1024 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10063

Description

The scan detected that the host is missing the following update:
ELSA-2019-1024

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008704.html

OEL7
x86_64
flatpak-1.0.2-5.el7_6
flatpak-devel-1.0.2-5.el7_6
flatpak-builder-1.0.0-5.el7_6
flatpak-libs-1.0.2-5.el7_6

163863 - Oracle Enterprise Linux ELSA-2019-1017 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3839, CVE-2019-6116

Description

The scan detected that the host is missing the following update:
ELSA-2019-1017

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008709.html
http://oss.oracle.com/pipermail/el-errata/2019-May/008703.html

OEL7
x86_64
ghostscript-gtk-9.07-31.el7_6.11
ghostscript-doc-9.07-31.el7_6.11
ghostscript-devel-9.07-31.el7_6.11
ghostscript-9.07-31.el7_6.11
ghostscript-cups-9.07-31.el7_6.11

186687 - Ubuntu Linux 18.04 USN-3981-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
USN-3981-1

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-May/004897.html

Ubuntu 18.04

linux-image-4.15.0-1039-aws_4.15.0-1039.41
linux-image-4.15.0-50-snapdragon_4.15.0-50.54
linux-image-aws_4.15.0.1039.38
linux-image-lowlatency_4.15.0.50.52
linux-image-4.15.0-1038-oem_4.15.0-1038.43
linux-image-powerpc-e500mc_4.15.0.50.52
linux-image-powerpc64-smp_4.15.0.50.52
linux-image-gcp_4.15.0.1032.34
linux-image-4.15.0-50-generic-lpae_4.15.0-50.54
linux-image-4.15.0-1034-kvm_4.15.0-1034.34
linux-image-4.15.0-50-lowlatency_4.15.0-50.54
linux-image-4.15.0-1013-oracle_4.15.0-1013.15
linux-image-4.15.0-1053-snapdragon_4.15.0-1053.57
linux-image-4.15.0-50-generic_4.15.0-50.54
linux-image-virtual_4.15.0.50.52
linux-image-powerpc-smp_4.15.0.50.52
linux-image-powerpc64-emb_4.15.0.50.52
linux-image-generic_4.15.0.50.52
linux-image-raspi2_4.15.0.1036.34
linux-image-4.15.0-1032-gcp_4.15.0-1032.34
linux-image-generic-lpae_4.15.0.50.52
linux-image-oracle_4.15.0.1013.16
linux-image-oem_4.15.0.1038.43
linux-image-kvm_4.15.0.1034.34
linux-image-4.15.0-1036-raspi2_4.15.0-1036.38
linux-image-snapdragon_4.15.0.1053.56

186700 - Ubuntu Linux 16.04 USN-3974-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11099, CVE-2018-11129, CVE-2018-11130

Description

The scan detected that the host is missing the following update:
USN-3974-1

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-May/004888.html

Ubuntu 16.04

vcftools_0.1.14+dfsg-2ubuntu0.1

186701 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3975-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698

Description

The scan detected that the host is missing the following update:
USN-3975-1

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-May/004889.html

Ubuntu 16.04

openjdk-8-jdk_8u212-b03-0ubuntu1.16.04.1
openjdk-8-jre_8u212-b03-0ubuntu1.16.04.1
openjdk-8-jre-jamvm_8u212-b03-0ubuntu1.16.04.1
openjdk-8-jdk-headless_8u212-b03-0ubuntu1.16.04.1
openjdk-8-jre-headless_8u212-b03-0ubuntu1.16.04.1

Ubuntu 18.10

openjdk-11-jre-headless_11.0.3+7-1ubuntu2~18.10.1
openjdk-11-jre_11.0.3+7-1ubuntu2~18.10.1
openjdk-11-jdk_11.0.3+7-1ubuntu2~18.10.1
openjdk-11-jdk-headless_11.0.3+7-1ubuntu2~18.10.1

Ubuntu 19.04

openjdk-11-jdk_11.0.3+7-1ubuntu2~19.04.1
openjdk-11-jre-headless_11.0.3+7-1ubuntu2~19.04.1
openjdk-11-jre_11.0.3+7-1ubuntu2~19.04.1

openjdk-11-jdk-headless_11.0.3+7-1ubuntu2~19.04.1

Ubuntu 18.04

openjdk-11-jdk_11.0.3+7-1ubuntu2~18.04.1
openjdk-11-jre_11.0.3+7-1ubuntu2~18.04.1
openjdk-11-jdk-headless_11.0.3+7-1ubuntu2~18.04.1
openjdk-11-jre-headless_11.0.3+7-1ubuntu2~18.04.1

186703 - Ubuntu Linux 14.04, 16.04 USN-3981-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
USN-3981-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-May/004903.html

Ubuntu 14.04

linux-image-azure_4.15.0.1045.32
linux-image-4.15.0-1045-azure_4.15.0-1045.49~14.04.1

Ubuntu 16.04

linux-image-4.15.0-50-lowlatency_4.15.0-50.54~16.04.1
linux-image-oracle_4.15.0.1013.7
linux-image-virtual-hwe-16.04_4.15.0.50.71
linux-image-4.15.0-1045-azure_4.15.0-1045.49
linux-image-generic-lpae-hwe-16.04_4.15.0.50.71
linux-image-4.15.0-50-generic_4.15.0-50.54~16.04.1
linux-image-4.15.0-1013-oracle_4.15.0-1013.15~16.04.1
linux-image-gcp_4.15.0.1032.46
linux-image-lowlatency-hwe-16.04_4.15.0.50.71
linux-image-4.15.0-1032-gcp_4.15.0-1032.34~16.04.1
linux-image-4.15.0-50-generic-lpae_4.15.0-50.54~16.04.1
linux-image-gke_4.15.0.1032.46
linux-image-azure_4.15.0.1045.49
linux-image-oem_4.15.0.50.71
linux-image-generic-hwe-16.04_4.15.0.50.71

186706 - Ubuntu Linux 18.04 USN-3980-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-3887, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
USN-3980-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-May/004900.html

Ubuntu 18.04

linux-image-4.18.0-20-lowlatency_4.18.0-20.21~18.04.1
linux-image-virtual-hwe-18.04_4.18.0.20.70
linux-image-4.18.0-20-snapdragon_4.18.0-20.21~18.04.1
linux-image-generic-hwe-18.04_4.18.0.20.70
linux-image-4.18.0-1018-azure_4.18.0-1018.18~18.04.1
linux-image-snapdragon-hwe-18.04_4.18.0.20.70
linux-image-lowlatency-hwe-18.04_4.18.0.20.70
linux-image-4.18.0-20-generic_4.18.0-20.21~18.04.1
linux-image-4.18.0-20-generic-lpae_4.18.0-20.21~18.04.1
linux-image-generic-lpae-hwe-18.04_4.18.0.20.70
linux-image-azure_4.18.0.1018.17

186707 - Ubuntu Linux 18.10 USN-3980-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-3887, CVE-2019-9500, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
USN-3980-1

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-May/004896.html

Ubuntu 18.10

linux-image-4.18.0-1016-aws_4.18.0-1016.18
linux-image-gcp_4.18.0.1011.11
linux-image-kvm_4.18.0.1012.12
linux-image-azure_4.18.0.1018.19
linux-image-powerpc64-smp_4.18.0.20.21
linux-image-powerpc64-emb_4.18.0.20.21
linux-image-4.18.0-1018-azure_4.18.0-1018.18
linux-image-4.18.0-20-generic_4.18.0-20.21
linux-image-4.18.0-20-generic-lpae_4.18.0-20.21
linux-image-4.18.0-20-lowlatency_4.18.0-20.21
linux-image-lowlatency_4.18.0.20.21
linux-image-powerpc-smp_4.18.0.20.21
linux-image-powerpc-e500mc_4.18.0.20.21
linux-image-snapdragon_4.18.0.20.21
linux-image-virtual_4.18.0.20.21

linux-image-4.18.0-1014-raspi2_4.18.0-1014.16
linux-image-4.18.0-20-snapdragon_4.18.0-20.21
linux-image-generic-lpae_4.18.0.20.21
linux-image-generic_4.18.0.20.21
linux-image-aws_4.18.0.1016.16
linux-image-raspi2_4.18.0.1014.11
linux-image-4.18.0-1011-gcp_4.18.0-1011.12
linux-image-gke_4.18.0.1011.11
linux-image-4.18.0-1012-kvm_4.18.0-1012.12

195157 - Fedora Linux 28 FEDORA-2019-d109db9c8a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5429

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d109db9c8a

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/2019/5/?count=200&page=3

Fedora Core 28

libfilezilla-0.15.1-1.fc28
filezilla-3.41.2-1.fc28

195163 - Fedora Linux 29 FEDORA-2019-6e325234a4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19935, CVE-2019-11036

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6e325234a4

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/2019/5/?count=200&page=2

Fedora Core 29

php-7.2.18-1.fc29

195167 - Fedora Linux 28 FEDORA-2019-bab3944fee Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19935, CVE-2019-11036

Description

The scan detected that the host is missing the following update:
FEDORA-2019-bab3944fee

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/2019/5/?count=200&page=2

Fedora Core 28

php-7.2.18-1.fc28

196313 - Red Hat Enterprise Linux RHSA-2019-1163 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10245, CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698

Description

The scan detected that the host is missing the following update:
RHSA-2019-1163

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00040.html

RHEL6D
x86_64
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el6_10

i386
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el6_10

RHEL6S
i386
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el6_10

x86_64
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el6_10

RHEL6WS
x86_64
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el6_10

i386
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el6_10
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el6_10

196317 - Red Hat Enterprise Linux RHSA-2019-1165 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10245, CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698

Description

The scan detected that the host is missing the following update:
RHSA-2019-1165

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00041.html

RHEL6D
x86_64
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el6_10

i386
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el6_10

RHEL6S
i386
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el6_10

x86_64
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el6_10

RHEL6WS
x86_64
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el6_10

i386
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el6_10

196326 - Red Hat Enterprise Linux RHSA-2019-1164 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10245, CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698

Description

The scan detected that the host is missing the following update:
RHSA-2019-1164

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00038.html

RHEL7D
x86_64
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el7

RHEL7S
x86_64
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el7

RHEL7WS
x86_64
java-1.8.0-ibm-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-demo-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-src-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.5.35-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.5.35-1jpp.1.el7

196330 - Red Hat Enterprise Linux RHSA-2019-1166 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10245, CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698

Description

The scan detected that the host is missing the following update:
RHSA-2019-1166

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-May/msg00039.html

RHEL7D
x86_64
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el7

RHEL7S
x86_64
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el7

RHEL7WS
x86_64
java-1.7.1-ibm-jdbc-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-devel-1.7.1.4.45-1jpp.1.el7

java-1.7.1-ibm-plugin-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-src-1.7.1.4.45-1jpp.1.el7
java-1.7.1-ibm-1.7.1.4.45-1jpp.1.el7

25091 - (MSPT-May2019) Microsoft Windows Improperly Handle Symbolic Links Privilege Escalation (CVE-2019-0936)

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

Risk Level: Medium

CVE: CVE-2019-0936

Description

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

Observation

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

The flaw lies due to improperly handle symbolic links. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25092 - (MSPT-May2019) Microsoft Storage Service Improperly Handles File Operations Privilege Escalation (CVE-2019-0931)

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

Risk Level: Medium

CVE: CVE-2019-0931

Description

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

Observation

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

The flaw lies due to improperly handles file operations. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25093 - (MSPT-May2019) Microsoft Windows Error Reporting Privilege Escalation (CVE-2019-0863)

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

Risk Level: Medium

CVE: CVE-2019-0863

Description

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

Observation

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

The flaw lies in the Error Reporting component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25094 - (MSPT-May2019) Microsoft Windows OLE Remote Code Execution (CVE-2019-0885)

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

Risk Level: Medium

CVE: CVE-2019-0885

Description

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

Observation

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

The flaw lies in the OLE component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25095 - (MSPT-May2019) Microsoft WDAC PowerShell Security Bypass (CVE-2019-0733)

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

Risk Level: Medium

CVE: CVE-2019-0733

Description

A vulnerability in some versions of Microsoft WDAC could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft WDAC could lead to security bypass.

The flaw lies in the WDAC component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to have valid credentials to the vulnerable system.

25096 - (MSPT-May2019) Microsoft Windows Unified Write Filter (UWF) Privilege Escalation (CVE-2019-0942)

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

Risk Level: Medium

CVE: CVE-2019-0942

Description

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

Observation

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

The flaw lies in the unified write filter (UWF) component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25097 - (MSPT-May2019) Microsoft Windows Hyper-V Information Disclosure (CVE-2019-0886)

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

Risk Level: Medium

CVE: CVE-2019-0886

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Hyper-V component.Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

25098 - (MSPT-May2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0758)

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

Risk Level: Medium

CVE: CVE-2019-0758

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the GDI component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

25099 - (MSPT-May2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0882)

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

Risk Level: Medium

CVE: CVE-2019-0882

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the GDI component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

25100 - (MSPT-May2019) Microsoft Windows GDI Remote Code Execution (CVE-2019-0903)

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

Risk Level: Medium

CVE: CVE-2019-0903

Description

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

Observation

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

The flaw lies in the GDI component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25101 - (MSPT-May2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0961)

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

Risk Level: Medium

CVE: CVE-2019-0961

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the gdi component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

25102 - (MSPT-May2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-0892)

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

Risk Level: Medium

CVE: CVE-2019-0892

Description

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

Observation

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

The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25104 - (MSPT-May2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0916)

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

Risk Level: Medium

CVE: CVE-2019-0916

Description

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

Observation

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

The flaw lies in the Chakra component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25105 - (MSPT-May2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0914)

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

Risk Level: Medium

CVE: CVE-2019-0914

Description

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

Observation

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

The flaw lies in the Chakra component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25106 - (MSPT-May2019) Microsoft Windows DHCP Remote Code Execution (CVE-2019-0725)

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

Risk Level: Medium

CVE: CVE-2019-0725

Description

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

Observation

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

The flaw lies in the DHCP component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

25107 - (MSPT-May2019) Microsoft NDIS ndis.sys Privilege Escalation (CVE-2019-0707)

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

Risk Level: Medium

CVE: CVE-2019-0707

Description

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

Observation

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

The flaw lies in the NDIS component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25108 - (MSPT-May2019) Microsoft Windows Remote Desktop Services Remote Code Execution (CVE-2019-0708)

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

Risk Level: Medium

CVE: CVE-2019-0708

Description

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

Observation

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

The flaw lies in the Remote Desktop Services component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

25110 - (MSPT-May2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0913)

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

Risk Level: Medium

CVE: CVE-2019-0913

Description

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

Observation

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

The flaw lies in the chakra scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25113 - (MSPT-May2019) Microsoft Windows Diagnostic Hub Standard Collector Privilege Escalation (CVE-2019-0727)

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

Risk Level: Medium

CVE: CVE-2019-0727

Description

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

Observation

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

The flaw lies in the Diagnostics Hub Standard Collector component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25114 - (MSPT-May2019) Microsoft Windows Kerberos Elevation of Privilege Vulnerability (CVE-2019-0734)

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

Risk Level: Medium

CVE: CVE-2019-0734

Description

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

Observation

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

The flaw lies in the Kerberos component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25115 - (MSPT-May2019) Microsoft Windows Kernel Privilege Escalation (CVE-2019-0881)

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

Risk Level: Medium

CVE: CVE-2019-0881

Description

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

Observation

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

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25116 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0889)

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

Risk Level: Medium

CVE: CVE-2019-0889

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25117 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0890)

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

Risk Level: Medium

CVE: CVE-2019-0890

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25118 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0891)

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

Risk Level: Medium

CVE: CVE-2019-0891

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25120 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0893)

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

Risk Level: Medium

CVE: CVE-2019-0893

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25121 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0894)

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

Risk Level: Medium

CVE: CVE-2019-0894

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25122 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0895)

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

Risk Level: Medium

CVE: CVE-2019-0895

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25123 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0896)

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

Risk Level: Medium

CVE: CVE-2019-0896

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25124 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0897)

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

Risk Level: Medium

CVE: CVE-2019-0897

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25125 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0898)

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

Risk Level: Medium

CVE: CVE-2019-0898

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25126 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0899)

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

Risk Level: Medium

CVE: CVE-2019-0899

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25127 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0900)

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

Risk Level: Medium

CVE: CVE-2019-0900

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25128 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0901)

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

Risk Level: Medium

CVE: CVE-2019-0901

Description

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

Observation

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

The flaw lies in the Jet Database Engine component.Successful exploitation by a remote attacker could result in the execution of

arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25129 - (MSPT-May2019) Microsoft Jet Database Engine Remote Code Execution (CVE-2019-0902)

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

Risk Level: Medium

CVE: CVE-2019-0902

Description

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

Observation

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

The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25130 - (MSPT-May2019) Microsoft SharePoint Server Improperly Sanitize Web Request Spoofing (CVE-2019-0949)

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

Risk Level: Medium

CVE: CVE-2019-0949

Description

A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing

The flaw lies due to improperly sanitize web request. Successful exploitation by an authenticated attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

25131 - (MSPT-May2019) Microsoft Azure DevOps Server Improperly Sanitize Authentication Request Information Disclosure (CVE-2019-0971)

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

Risk Level: Medium

CVE: CVE-2019-0971

Description

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to information disclosure.

The flaw is due to improper handling of a specially crafted authentication request. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

25133 - (MSPT-May2019) Microsoft SharePoint Server Improperly Sanitize Web Request Spoofing (CVE-2019-0950)

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

Risk Level: Medium

CVE: CVE-2019-0950

Description

A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

The flaw is due to improper handling of a specially crafted web request. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

25134 - (MSPT-May2019) Microsoft SharePoint Server Improperly Sanitize Web Request Spoofing (CVE-2019-0951)

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

Risk Level: Medium

CVE: CVE-2019-0951

Description

A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

The flaw is due to improper handling of a specially crafted web request. Successful exploitation by an authenticated attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

25136 - (MSPT-May2019) Microsoft SharePoint Server Information Disclosure (CVE-2019-0956)

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

Risk Level: Medium

CVE: CVE-2019-0956

Description

A vulnerability in some versions of Microsoft SharePoint Server could lead to information disclosure

Observation

A vulnerability in some versions of Microsoft SharePoint Server could lead to information disclosure.

The flaw is due to improper handling of a specially crafted web request. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

25137 - (MSPT-May2019) Microsoft SharePoint Elevation of Privilege (CVE-2019-0957)

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

Risk Level: Medium

CVE: CVE-2019-0957

Description

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

Observation

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

The flaw is due to improper handling of a specially crafted web request. Successful exploitation could allow an authenticated attacker to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

25138 - (MSPT-May2019) Microsoft SharePoint Elevation of Privilege (CVE-2019-0958)

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

Risk Level: Medium

CVE: CVE-2019-0958

Description

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

Observation

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

The flaw is due to improper handling of a specially crafted web request. Successful exploitation could allow an authenticated attacker to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

25146 - (MSPT-May2019) Microsoft Azure AD Connect Privilege Escalation (CVE-2019-1000)

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

Risk Level: Medium

CVE: CVE-2019-1000

Description

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

Observation

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

The flaw lies in the build 1.3.20.0. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25153 - (MSPT-May2019) Microsoft .NET Framework Denial of Service (CVE-2019-0864)

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

Risk Level: Medium

CVE: CVE-2019-0864

Description

A vulnerability in some versions of Microsoft .NET Framework could lead to denial of service.

Observation

A vulnerability in some versions of Microsoft .NET Framework could lead to denial of service.

The flaw is due to improper handling of objects in heap memory. Successful exploitation by a remote attacker could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.

25155 - (MSPT-May2019) Microsoft Internet Explorer Improperly Handles URLs Spoofing (CVE-2019-0921)

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

Risk Level: Medium

CVE: CVE-2019-0921

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to spoofing.

The flaw lies due to improperly handles urls. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

25156 - (MSPT-May2019) Microsoft Internet Explorer Improperly Handles Objects in Memory Information Disclosure (CVE-2019-0930)

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

Risk Level: Medium

CVE: CVE-2019-0930

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to information disclosure.

The flaw lies due to improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

25159 - (MSPT-May2019) Microsoft Browsers Scripting Engine Remote Code Execution (CVE-2019-0884)

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

Risk Level: Medium

CVE: CVE-2019-0884

Description

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

Observation

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25166 - (MSPT-May2019) Microsoft Edge AppContainer Privilege Escalation (CVE-2019-0938)

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

Risk Level: Medium

CVE: CVE-2019-0938

Description

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

Observation

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

The flaw lies in the AppContainer component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

25171 - (MSPT-May2019) Microsoft SQL Server Analysis Services Information Disclosure (CVE-2019-0819)

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

Risk Level: Medium

CVE: CVE-2019-0819

Description

A vulnerability in some versions of Microsoft SQL Server could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft SQL Server could lead to information disclosure.

The flaw lies in the Analysis Services component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

25175 - (MSPT-May2019) Microsoft Dynamics On Premise Security Bypass (CVE-2019-1008)

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

Risk Level: Medium

CVE: CVE-2019-1008

Description

A vulnerability in some versions of Microsoft Dynamics could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Dynamics could lead to security bypass.

The flaw lies in the On-Premise component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions.

131343 - Debian Linux 9.0 DSA-4441-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14773, CVE-2018-19789, CVE-2018-19790, CVE-2019-10909, CVE-2019-10910, CVE-2019-10911, CVE-2019-10912, CVE-2019-10913

Description

The scan detected that the host is missing the following update:
DSA-4441-1

Observation

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

http://www.debian.org/security/2019/dsa-4441

Debian 9.0
all
php-symfony-twig-bundle_2.8.7+dfsg-1.3+deb9u2
php-symfony-finder_2.8.7+dfsg-1.3+deb9u2
php-symfony-security-http_2.8.7+dfsg-1.3+deb9u2
php-symfony-phpunit-bridge_2.8.7+dfsg-1.3+deb9u2
php-symfony-options-resolver_2.8.7+dfsg-1.3+deb9u2
php-symfony-class-loader_2.8.7+dfsg-1.3+deb9u2
php-symfony-dependency-injection_2.8.7+dfsg-1.3+deb9u2
php-symfony-monolog-bridge_2.8.7+dfsg-1.3+deb9u2
php-symfony-security-guard_2.8.7+dfsg-1.3+deb9u2
php-symfony-intl_2.8.7+dfsg-1.3+deb9u2
php-symfony-asset_2.8.7+dfsg-1.3+deb9u2
php-symfony-security-csrf_2.8.7+dfsg-1.3+deb9u2
php-symfony-serializer_2.8.7+dfsg-1.3+deb9u2
php-symfony-proxy-manager-bridge_2.8.7+dfsg-1.3+deb9u2
php-symfony-routing_2.8.7+dfsg-1.3+deb9u2
php-symfony-framework-bundle_2.8.7+dfsg-1.3+deb9u2
php-symfony-swiftmailer-bridge_2.8.7+dfsg-1.3+deb9u2
php-symfony-debug-bundle_2.8.7+dfsg-1.3+deb9u2
php-symfony-security-core_2.8.7+dfsg-1.3+deb9u2
php-symfony-event-dispatcher_2.8.7+dfsg-1.3+deb9u2
php-symfony-web-profiler-bundle_2.8.7+dfsg-1.3+deb9u2
php-symfony-twig-bridge_2.8.7+dfsg-1.3+deb9u2
php-symfony-console_2.8.7+dfsg-1.3+deb9u2
php-symfony-http-foundation_2.8.7+dfsg-1.3+deb9u2
php-symfony-locale_2.8.7+dfsg-1.3+deb9u2
php-symfony-debug_2.8.7+dfsg-1.3+deb9u2
php-symfony_2.8.7+dfsg-1.3+deb9u2
php-symfony-http-kernel_2.8.7+dfsg-1.3+deb9u2
php-symfony-filesystem_2.8.7+dfsg-1.3+deb9u2
php-symfony-property-access_2.8.7+dfsg-1.3+deb9u2
php-symfony-translation_2.8.7+dfsg-1.3+deb9u2
php-symfony-ldap_2.8.7+dfsg-1.3+deb9u2
php-symfony-form_2.8.7+dfsg-1.3+deb9u2
php-symfony-property-info_2.8.7+dfsg-1.3+deb9u2
php-symfony-browser-kit_2.8.7+dfsg-1.3+deb9u2
php-symfony-security_2.8.7+dfsg-1.3+deb9u2
php-symfony-process_2.8.7+dfsg-1.3+deb9u2
php-symfony-yaml_2.8.7+dfsg-1.3+deb9u2
php-symfony-stopwatch_2.8.7+dfsg-1.3+deb9u2
php-symfony-templating_2.8.7+dfsg-1.3+deb9u2
php-symfony-var-dumper_2.8.7+dfsg-1.3+deb9u2
php-symfony-validator_2.8.7+dfsg-1.3+deb9u2
php-symfony-config_2.8.7+dfsg-1.3+deb9u2
php-symfony-css-selector_2.8.7+dfsg-1.3+deb9u2

php-symfony-security-bundle_2.8.7+dfsg-1.3+deb9u2
php-symfony-expression-language_2.8.7+dfsg-1.3+deb9u2
php-symfony-dom-crawler_2.8.7+dfsg-1.3+deb9u2
php-symfony-doctrine-bridge_2.8.7+dfsg-1.3+deb9u2

147918 - SuSE Linux 15.0 openSUSE-SU-2019:1353-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16868, CVE-2019-3829, CVE-2019-3836

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1353-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00049.html

SuSE Linux 15.0
x86_64
libgnutls-dane0-3.6.7-lp150.9.1
libgnutls-dane-devel-3.6.7-lp150.9.1
libgnutls-devel-32bit-3.6.7-lp150.9.1
gnutls-guile-debuginfo-3.6.7-lp150.9.1
libgnutls30-32bit-3.6.7-lp150.9.1
gnutls-3.6.7-lp150.9.1
libgnutls30-32bit-debuginfo-3.6.7-lp150.9.1
libgnutlsxx28-3.6.7-lp150.9.1
libgnutls30-3.6.7-lp150.9.1
gnutls-debugsource-3.6.7-lp150.9.1
gnutls-debuginfo-3.6.7-lp150.9.1
libgnutls-dane0-debuginfo-3.6.7-lp150.9.1
libgnutls30-debuginfo-3.6.7-lp150.9.1
libgnutlsxx28-debuginfo-3.6.7-lp150.9.1
libgnutls-devel-3.6.7-lp150.9.1
gnutls-guile-3.6.7-lp150.9.1
libgnutlsxx-devel-3.6.7-lp150.9.1

i586
libgnutls-dane0-3.6.7-lp150.9.1
libgnutls-dane-devel-3.6.7-lp150.9.1
gnutls-guile-debuginfo-3.6.7-lp150.9.1
gnutls-3.6.7-lp150.9.1
libgnutlsxx28-3.6.7-lp150.9.1
libgnutls30-3.6.7-lp150.9.1
gnutls-debugsource-3.6.7-lp150.9.1
gnutls-debuginfo-3.6.7-lp150.9.1
libgnutls-dane0-debuginfo-3.6.7-lp150.9.1
libgnutls30-debuginfo-3.6.7-lp150.9.1
libgnutlsxx28-debuginfo-3.6.7-lp150.9.1
libgnutls-devel-3.6.7-lp150.9.1
gnutls-guile-3.6.7-lp150.9.1
libgnutlsxx-devel-3.6.7-lp150.9.1

147923 - SuSE Linux 15.0 openSUSE-SU-2019:1372-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9936, CVE-2019-9937

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1372-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00074.html

SuSE Linux 15.0
i586
libsqlite3-0-3.28.0-lp150.2.6.1
sqlite3-debuginfo-3.28.0-lp150.2.6.1
libsqlite3-0-debuginfo-3.28.0-lp150.2.6.1
sqlite3-3.28.0-lp150.2.6.1
sqlite3-devel-3.28.0-lp150.2.6.1
sqlite3-debugsource-3.28.0-lp150.2.6.1

noarch
sqlite3-doc-3.28.0-lp150.2.6.1

x86_64
libsqlite3-0-3.28.0-lp150.2.6.1
libsqlite3-0-32bit-debuginfo-3.28.0-lp150.2.6.1
sqlite3-debuginfo-3.28.0-lp150.2.6.1
libsqlite3-0-debuginfo-3.28.0-lp150.2.6.1
sqlite3-3.28.0-lp150.2.6.1
sqlite3-devel-3.28.0-lp150.2.6.1
sqlite3-debugsource-3.28.0-lp150.2.6.1
libsqlite3-0-32bit-3.28.0-lp150.2.6.1

147924 - SuSE Linux 42.3 openSUSE-SU-2019:1392-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15173

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1392-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00084.html

SuSE Linux 42.3
x86_64

nmap-6.47-13.3.1
zenmap-6.47-13.3.1
nmap-debuginfo-6.47-13.3.1
ndiff-6.47-13.3.1
ncat-6.47-13.3.1
nping-6.47-13.3.1
nmap-debugsource-6.47-13.3.1

i586
nmap-6.47-13.3.1
zenmap-6.47-13.3.1
nmap-debuginfo-6.47-13.3.1
ndiff-6.47-13.3.1
ncat-6.47-13.3.1
nping-6.47-13.3.1
nmap-debugsource-6.47-13.3.1

147925 - SuSE Linux 42.3 openSUSE-SU-2019:1371-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1371-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00072.html

SuSE Linux 42.3
x86_64
python3-debugsource-3.4.6-12.10.2
libpython3_4m1_0-debuginfo-3.4.6-12.10.1
python3-testsuite-3.4.6-12.10.1
python3-testsuite-debuginfo-3.4.6-12.10.1
python3-tk-debuginfo-3.4.6-12.10.2
python3-32bit-3.4.6-12.10.2
python3-dbm-3.4.6-12.10.2
python3-idle-3.4.6-12.10.1
libpython3_4m1_0-32bit-3.4.6-12.10.1
python3-tk-3.4.6-12.10.2
python3-dbm-debuginfo-3.4.6-12.10.2
python3-base-32bit-3.4.6-12.10.1
python3-base-debuginfo-3.4.6-12.10.1
libpython3_4m1_0-3.4.6-12.10.1
python3-debuginfo-3.4.6-12.10.2
libpython3_4m1_0-debuginfo-32bit-3.4.6-12.10.1
python3-debuginfo-32bit-3.4.6-12.10.2
python3-base-debuginfo-32bit-3.4.6-12.10.1
python3-curses-3.4.6-12.10.2
python3-devel-3.4.6-12.10.1
python3-tools-3.4.6-12.10.1
python3-3.4.6-12.10.2
python3-devel-debuginfo-3.4.6-12.10.1

python3-base-debugsource-3.4.6-12.10.1
python3-curses-debuginfo-3.4.6-12.10.2
python3-base-3.4.6-12.10.1

i586
python3-debugsource-3.4.6-12.10.2
libpython3_4m1_0-debuginfo-3.4.6-12.10.1
python3-testsuite-3.4.6-12.10.1
python3-testsuite-debuginfo-3.4.6-12.10.1
python3-tk-debuginfo-3.4.6-12.10.2
python3-dbm-3.4.6-12.10.2
python3-idle-3.4.6-12.10.1
python3-tk-3.4.6-12.10.2
python3-dbm-debuginfo-3.4.6-12.10.2
python3-base-debuginfo-3.4.6-12.10.1
libpython3_4m1_0-3.4.6-12.10.1
python3-debuginfo-3.4.6-12.10.2
python3-curses-3.4.6-12.10.2
python3-devel-3.4.6-12.10.1
python3-tools-3.4.6-12.10.1
python3-3.4.6-12.10.2
python3-devel-debuginfo-3.4.6-12.10.1
python3-base-debugsource-3.4.6-12.10.1
python3-curses-debuginfo-3.4.6-12.10.2
python3-base-3.4.6-12.10.1

147926 - SuSE Linux 42.3 openSUSE-SU-2019:1391-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11070, CVE-2019-6201, CVE-2019-6251, CVE-2019-7285, CVE-2019-7292, CVE-2019-8503, CVE-2019-8506, CVE-2019-8515, CVE-2019-8524, CVE-2019-8535, CVE-2019-8536, CVE-2019-8544, CVE-2019-8551, CVE-2019-8558, CVE-2019-8559, CVE-2019-8563

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1391-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00088.html

SuSE Linux 42.3
i586
webkit2gtk3-debugsource-2.24.1-27.1
webkit-jsc-4-2.24.1-27.1
libjavascriptcoregtk-4_0-18-2.24.1-27.1
webkit2gtk3-minibrowser-debuginfo-2.24.1-27.1
webkit2gtk3-minibrowser-2.24.1-27.1
webkit2gtk-4_0-injected-bundles-2.24.1-27.1
webkit2gtk3-devel-2.24.1-27.1
webkit-jsc-4-debuginfo-2.24.1-27.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-27.1
typelib-1_0-WebKit2-4_0-2.24.1-27.1
webkit2gtk3-plugin-process-gtk2-2.24.1-27.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-27.1

typelib-1_0-WebKit2WebExtension-4_0-2.24.1-27.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.1-27.1
libwebkit2gtk-4_0-37-2.24.1-27.1
typelib-1_0-JavaScriptCore-4_0-2.24.1-27.1
libwebkit2gtk-4_0-37-debuginfo-2.24.1-27.1

noarch
libwebkit2gtk3-lang-2.24.1-27.1

x86_64
webkit2gtk3-debugsource-2.24.1-27.1
libjavascriptcoregtk-4_0-18-32bit-2.24.1-27.1
webkit-jsc-4-2.24.1-27.1
libwebkit2gtk-4_0-37-32bit-2.24.1-27.1
libjavascriptcoregtk-4_0-18-2.24.1-27.1
libwebkit2gtk-4_0-37-debuginfo-32bit-2.24.1-27.1
webkit2gtk3-minibrowser-debuginfo-2.24.1-27.1
webkit2gtk3-minibrowser-2.24.1-27.1
webkit2gtk-4_0-injected-bundles-2.24.1-27.1
webkit2gtk3-devel-2.24.1-27.1
webkit-jsc-4-debuginfo-2.24.1-27.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-27.1
typelib-1_0-WebKit2-4_0-2.24.1-27.1
libjavascriptcoregtk-4_0-18-debuginfo-32bit-2.24.1-27.1
webkit2gtk3-plugin-process-gtk2-2.24.1-27.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-27.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.1-27.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.1-27.1
libwebkit2gtk-4_0-37-2.24.1-27.1
typelib-1_0-JavaScriptCore-4_0-2.24.1-27.1
libwebkit2gtk-4_0-37-debuginfo-2.24.1-27.1

147927 - SuSE Linux 15.0 openSUSE-SU-2019:1356-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10899, CVE-2019-10901, CVE-2019-10903

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1356-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00056.html

SuSE Linux 15.0
x86_64
libwscodecs1-debuginfo-2.4.14-lp150.2.26.3
libwireshark9-debuginfo-2.4.14-lp150.2.26.3
libwsutil8-2.4.14-lp150.2.26.3
wireshark-ui-qt-2.4.14-lp150.2.26.3
wireshark-debuginfo-2.4.14-lp150.2.26.3
wireshark-ui-qt-debuginfo-2.4.14-lp150.2.26.3
wireshark-devel-2.4.14-lp150.2.26.3
wireshark-2.4.14-lp150.2.26.3

wireshark-debugsource-2.4.14-lp150.2.26.3
libwsutil8-debuginfo-2.4.14-lp150.2.26.3
libwiretap7-2.4.14-lp150.2.26.3
libwscodecs1-2.4.14-lp150.2.26.3
libwiretap7-debuginfo-2.4.14-lp150.2.26.3
libwireshark9-2.4.14-lp150.2.26.3

i586
libwscodecs1-debuginfo-2.4.14-lp150.2.26.3
libwireshark9-debuginfo-2.4.14-lp150.2.26.3
libwsutil8-2.4.14-lp150.2.26.3
wireshark-ui-qt-2.4.14-lp150.2.26.3
wireshark-debuginfo-2.4.14-lp150.2.26.3
wireshark-ui-qt-debuginfo-2.4.14-lp150.2.26.3
wireshark-devel-2.4.14-lp150.2.26.3
wireshark-2.4.14-lp150.2.26.3
wireshark-debugsource-2.4.14-lp150.2.26.3
libwsutil8-debuginfo-2.4.14-lp150.2.26.3
libwiretap7-2.4.14-lp150.2.26.3
libwscodecs1-2.4.14-lp150.2.26.3
libwiretap7-debuginfo-2.4.14-lp150.2.26.3
libwireshark9-2.4.14-lp150.2.26.3

147928 - SuSE Linux 42.3 openSUSE-SU-2019:1390-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10899, CVE-2019-10901, CVE-2019-10903, CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1390-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00080.html

SuSE Linux 42.3
x86_64
libwiretap7-debuginfo-2.4.14-52.1
libwscodecs1-debuginfo-2.4.14-52.1
wireshark-debuginfo-2.4.14-52.1
libwireshark9-debuginfo-2.4.14-52.1
wireshark-devel-2.4.14-52.1
libwireshark9-2.4.14-52.1
wireshark-gtk-debuginfo-2.4.14-52.1
libwscodecs1-2.4.14-52.1
libwsutil8-debuginfo-2.4.14-52.1
libwsutil8-2.4.14-52.1
wireshark-gtk-2.4.14-52.1
wireshark-ui-qt-2.4.14-52.1
wireshark-debugsource-2.4.14-52.1
wireshark-2.4.14-52.1
wireshark-ui-qt-debuginfo-2.4.14-52.1
libwiretap7-2.4.14-52.1

147933 - SuSE Linux 15.0 openSUSE-SU-2019:1374-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11070, CVE-2019-6201, CVE-2019-6251, CVE-2019-7285, CVE-2019-7292, CVE-2019-8503, CVE-2019-8506, CVE-2019-8515, CVE-2019-8518, CVE-2019-8523, CVE-2019-8524, CVE-2019-8535, CVE-2019-8536, CVE-2019-8544, CVE-2019-8551, CVE-2019-8558, CVE-2019-8559, CVE-2019-8563

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1374-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00073.html

SuSE Linux 15.0
i586
webkit2gtk3-plugin-process-gtk2-2.24.1-lp150.2.19.1
libwebkit2gtk-4_0-37-2.24.1-lp150.2.19.1
typelib-1_0-JavaScriptCore-4_0-2.24.1-lp150.2.19.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.1-lp150.2.19.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-devel-2.24.1-lp150.2.19.1
libjavascriptcoregtk-4_0-18-2.24.1-lp150.2.19.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-minibrowser-2.24.1-lp150.2.19.1
libwebkit2gtk-4_0-37-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-debugsource-2.24.1-lp150.2.19.1
webkit2gtk3-minibrowser-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.1-lp150.2.19.1
typelib-1_0-WebKit2-4_0-2.24.1-lp150.2.19.1
webkit2gtk-4_0-injected-bundles-2.24.1-lp150.2.19.1
webkit-jsc-4-2.24.1-lp150.2.19.1
webkit-jsc-4-debuginfo-2.24.1-lp150.2.19.1

noarch
libwebkit2gtk3-lang-2.24.1-lp150.2.19.1

x86_64
libwebkit2gtk-4_0-37-32bit-2.24.1-lp150.2.19.1
libjavascriptcoregtk-4_0-18-32bit-2.24.1-lp150.2.19.1
webkit2gtk3-plugin-process-gtk2-2.24.1-lp150.2.19.1
libwebkit2gtk-4_0-37-2.24.1-lp150.2.19.1
typelib-1_0-JavaScriptCore-4_0-2.24.1-lp150.2.19.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.1-lp150.2.19.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-devel-2.24.1-lp150.2.19.1
libjavascriptcoregtk-4_0-18-2.24.1-lp150.2.19.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-lp150.2.19.1
libjavascriptcoregtk-4_0-18-32bit-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-minibrowser-2.24.1-lp150.2.19.1
libwebkit2gtk-4_0-37-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-debugsource-2.24.1-lp150.2.19.1
webkit2gtk3-minibrowser-debuginfo-2.24.1-lp150.2.19.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.1-lp150.2.19.1

typelib-1_0-WebKit2-4_0-2.24.1-lp150.2.19.1
webkit2gtk-4_0-injected-bundles-2.24.1-lp150.2.19.1
webkit-jsc-4-2.24.1-lp150.2.19.1
webkit-jsc-4-debuginfo-2.24.1-lp150.2.19.1
libwebkit2gtk-4_0-37-32bit-debuginfo-2.24.1-lp150.2.19.1

147939 - SuSE Linux 42.3 openSUSE-SU-2019:1343-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1152, CVE-2018-11813, CVE-2018-14498

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1343-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00045.html

SuSE Linux 42.3
x86_64
libjpeg-turbo-debugsource-1.5.3-45.1
libjpeg62-turbo-1.5.3-45.1
libjpeg62-turbo-debugsource-1.5.3-45.1
libjpeg8-8.1.2-45.1
libjpeg8-debuginfo-8.1.2-45.1
libjpeg62-devel-62.2.0-45.1
libjpeg8-devel-32bit-8.1.2-45.1
libjpeg62-devel-32bit-62.2.0-45.1
libturbojpeg0-8.1.2-45.1
libturbojpeg0-32bit-8.1.2-45.1
libjpeg62-32bit-62.2.0-45.1
libjpeg-turbo-1.5.3-45.1
libturbojpeg0-debuginfo-32bit-8.1.2-45.1
libjpeg62-62.2.0-45.1
libjpeg-turbo-debuginfo-1.5.3-45.1
libturbojpeg0-debuginfo-8.1.2-45.1
libjpeg8-devel-8.1.2-45.1
libjpeg8-32bit-8.1.2-45.1
libjpeg62-debuginfo-32bit-62.2.0-45.1
libjpeg62-debuginfo-62.2.0-45.1
libjpeg8-debuginfo-32bit-8.1.2-45.1

i586
libjpeg-turbo-debugsource-1.5.3-45.1
libjpeg62-turbo-1.5.3-45.1
libjpeg62-turbo-debugsource-1.5.3-45.1
libjpeg8-8.1.2-45.1
libjpeg8-debuginfo-8.1.2-45.1
libjpeg62-devel-62.2.0-45.1
libturbojpeg0-8.1.2-45.1
libjpeg-turbo-1.5.3-45.1
libjpeg62-62.2.0-45.1
libjpeg-turbo-debuginfo-1.5.3-45.1
libturbojpeg0-debuginfo-8.1.2-45.1

libjpeg8-devel-8.1.2-45.1
libjpeg62-debuginfo-62.2.0-45.1

160557 - CentOS 7 CESA-2019-1022 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10745

Description

The scan detected that the host is missing the following update:
CESA-2019-1022

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-May/023303.html

CentOS 7
noarch
python-jinja2-2.7.2-3.el7_6

163859 - Oracle Enterprise Linux ELSA-2019-1022 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10745

Description

The scan detected that the host is missing the following update:
ELSA-2019-1022

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-May/008705.html
http://oss.oracle.com/pipermail/el-errata/2019-May/008712.html

OEL7
x86_64
python-jinja2-2.7.2-3.el7_6

186697 - Ubuntu Linux 18.10, 19.04 USN-3971-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11454, CVE-2019-11455

Description

The scan detected that the host is missing the following update:
USN-3971-1

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-May/004883.html

Ubuntu 19.04

monit_5.25.2-3ubuntu0.1

Ubuntu 18.10

monit_5.25.2-1ubuntu0.1

186702 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10, 19.04 USN-3978-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-20815, CVE-2019-11091, CVE-2019-5008, CVE-2019-9824

Description

The scan detected that the host is missing the following update:
USN-3978-1

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-May/004893.html

Ubuntu 16.04

qemu_2.5+dfsg-5ubuntu10.38
qemu-system-x86_2.5+dfsg-5ubuntu10.38

Ubuntu 18.10

qemu_2.12+dfsg-3ubuntu8.7
qemu-system-x86_2.12+dfsg-3ubuntu8.7

Ubuntu 19.04

qemu_3.1+dfsg-2ubuntu3.1
qemu-system-x86_3.1+dfsg-2ubuntu3.1

Ubuntu 14.04

qemu_2.0.0+dfsg-2ubuntu1.46
qemu-system-x86_2.0.0+dfsg-2ubuntu1.46

Ubuntu 18.04

qemu-system-x86_2.11+dfsg-1ubuntu7.13
qemu_2.11+dfsg-1ubuntu7.13

195153 - Fedora Linux 30 FEDORA-2019-7813edd5a2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3110, CVE-2016-8612

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7813edd5a2

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/2019/5/?count=200&page=3

Fedora Core 30

mod_cluster-1.3.11-1.fc30

195155 - Fedora Linux 29 FEDORA-2019-17556e2ad6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3110, CVE-2016-8612

Description

The scan detected that the host is missing the following update:
FEDORA-2019-17556e2ad6

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/2019/5/?count=200&page=3

Fedora Core 29

mod_cluster-1.3.11-1.fc29

195159 - Fedora Linux 28 FEDORA-2019-3877efca99 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3110, CVE-2016-8612

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3877efca99

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/2019/5/?count=200&page=3

Fedora Core 28

mod_cluster-1.3.11-1.fc28

195169 - Fedora Linux 29 FEDORA-2019-a06dffab1c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2922, CVE-2019-11358

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a06dffab1c

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/2019/5/?count=200&page=3

Fedora Core 29

drupal7-7.66-1.fc29

147941 - SuSE Linux 42.3 openSUSE-SU-2019:1342-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16877, CVE-2018-16878

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1342-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00042.html

SuSE Linux 42.3
x86_64
pacemaker-remote-1.1.16-4.12.1
pacemaker-cts-debuginfo-1.1.16-4.12.1
libpacemaker3-1.1.16-4.12.1
pacemaker-debuginfo-1.1.16-4.12.1
pacemaker-1.1.16-4.12.1
pacemaker-cts-1.1.16-4.12.1
pacemaker-cli-debuginfo-1.1.16-4.12.1
libpacemaker3-debuginfo-1.1.16-4.12.1
pacemaker-remote-debuginfo-1.1.16-4.12.1
pacemaker-cli-1.1.16-4.12.1
libpacemaker-devel-1.1.16-4.12.1
pacemaker-debugsource-1.1.16-4.12.1

i586

pacemaker-remote-1.1.16-4.12.1
pacemaker-cts-debuginfo-1.1.16-4.12.1
libpacemaker3-1.1.16-4.12.1
pacemaker-debuginfo-1.1.16-4.12.1
pacemaker-1.1.16-4.12.1
pacemaker-cts-1.1.16-4.12.1
pacemaker-cli-debuginfo-1.1.16-4.12.1
libpacemaker3-debuginfo-1.1.16-4.12.1
pacemaker-remote-debuginfo-1.1.16-4.12.1
pacemaker-cli-1.1.16-4.12.1
libpacemaker-devel-1.1.16-4.12.1
pacemaker-debugsource-1.1.16-4.12.1

186691 - Ubuntu Linux 16.04 USN-3982-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882

Description

The scan detected that the host is missing the following update:
USN-3982-1

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-May/004898.html

Ubuntu 16.04

linux-image-aws_4.4.0.1083.86
linux-image-4.4.0-148-powerpc-e500mc_4.4.0-148.174
linux-image-powerpc-smp_4.4.0.148.156
linux-image-4.4.0-1046-kvm_4.4.0-1046.52
linux-image-snapdragon_4.4.0.1113.105
linux-image-generic-lpae_4.4.0.148.156
linux-image-lowlatency_4.4.0.148.156
linux-image-4.4.0-1083-aws_4.4.0-1083.93
linux-image-4.4.0-148-powerpc64-smp_4.4.0-148.174
linux-image-powerpc-e500mc_4.4.0.148.156
linux-image-virtual_4.4.0.148.156
linux-image-generic_4.4.0.148.156
linux-image-4.4.0-1113-snapdragon_4.4.0-1113.118
linux-image-4.4.0-148-powerpc64-emb_4.4.0-148.174
linux-image-4.4.0-148-lowlatency_4.4.0-148.174
linux-image-4.4.0-148-generic-lpae_4.4.0-148.174
linux-image-kvm_4.4.0.1046.46
linux-image-4.4.0-148-powerpc-smp_4.4.0-148.174
linux-image-raspi2_4.4.0.1109.109
linux-image-powerpc64-smp_4.4.0.148.156
linux-image-4.4.0-1109-raspi2_4.4.0-1109.117
linux-image-powerpc64-emb_4.4.0.148.156
linux-image-4.4.0-148-generic_4.4.0-148.174

186699 - Ubuntu Linux 14.04 USN-3982-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882

Description

The scan detected that the host is missing the following update:
USN-3982-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-May/004901.html

Ubuntu 14.04

linux-image-4.4.0-148-lowlatency_4.4.0-148.174~14.04.1
linux-image-generic-lts-xenial_4.4.0.148.130
linux-image-generic-lpae-lts-xenial_4.4.0.148.130
linux-image-powerpc64-emb-lts-xenial_4.4.0.148.130
linux-image-4.4.0-148-generic-lpae_4.4.0-148.174~14.04.1
linux-image-virtual-lts-xenial_4.4.0.148.130
linux-image-4.4.0-148-powerpc-e500mc_4.4.0-148.174~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.148.130
linux-image-4.4.0-148-powerpc-smp_4.4.0-148.174~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.148.130
linux-image-powerpc-smp-lts-xenial_4.4.0.148.130
linux-image-4.4.0-148-powerpc64-emb_4.4.0-148.174~14.04.1
linux-image-4.4.0-148-generic_4.4.0-148.174~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.148.130
linux-image-4.4.0-148-powerpc64-smp_4.4.0-148.174~14.04.1

195164 - Fedora Linux 29 FEDORA-2019-7eaf0bbe7c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10909, CVE-2019-10910, CVE-2019-10911, CVE-2019-11358

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7eaf0bbe7c

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/2019/5/?count=200&page=3

Fedora Core 29

drupal8-8.6.15-1.fc29

195168 - Fedora Linux 30 FEDORA-2019-ff1b728d09 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11555

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ff1b728d09

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/2019/5/?count=200&page=1

Fedora Core 30

wpa_supplicant-2.8-2.fc30

195171 - Fedora Linux 30 FEDORA-2019-2a0ce0c58c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11358

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2a0ce0c58c

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/2019/5/?count=200&page=3

Fedora Core 30

drupal7-7.66-1.fc30

131342 - Debian Linux 9.0 DSA-4440-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5743, CVE-2018-5745, CVE-2019-6465

Description

The scan detected that the host is missing the following update:
DSA-4440-1

Observation

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

http://www.debian.org/security/2019/dsa-4440

Debian 9.0
all
bind9_1:9.10.3.dfsg.P4-12.3+deb9u5

131344 - Debian Linux 9.0 DSA-4439-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-10130

Description

The scan detected that the host is missing the following update:
DSA-4439-1

Observation

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

http://www.debian.org/security/2019/dsa-4439

Debian 9.0
all
postgresql-9.6_9.6.13-0+deb9u1

131345 - Debian Linux 9.0 DSA-4442-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3839

Description

The scan detected that the host is missing the following update:
DSA-4442-1

Observation

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

http://www.debian.org/security/2019/dsa-4442

Debian 9.0
all
ghostscript_9.26a~dfsg-0+deb9u3

147944 - SuSE Linux 42.3 openSUSE-SU-2019:1345-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-14526

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1345-1

Observation

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

For more information see:

https://lists.opensuse.org/opensuse-updates/2019-05/msg00043.html

SuSE Linux 42.3
x86_64
wpa_supplicant-2.6-16.1
wpa_supplicant-debuginfo-2.6-16.1
wpa_supplicant-debugsource-2.6-16.1
wpa_supplicant-gui-debuginfo-2.6-16.1
wpa_supplicant-gui-2.6-16.1

i586
wpa_supplicant-2.6-16.1
wpa_supplicant-debuginfo-2.6-16.1
wpa_supplicant-debugsource-2.6-16.1
wpa_supplicant-gui-debuginfo-2.6-16.1
wpa_supplicant-gui-2.6-16.1

186686 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3976-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-16860

Description

The scan detected that the host is missing the following update:
USN-3976-1

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-May/004890.html

Ubuntu 16.04

samba_4.3.11+dfsg-0ubuntu0.16.04.20

Ubuntu 18.10

samba_4.8.4+dfsg-2ubuntu2.4

Ubuntu 19.04

samba_4.10.0+dfsg-0ubuntu2.1

Ubuntu 18.04

samba_4.7.6+dfsg~ubuntu-0ubuntu2.10

186688 - Ubuntu Linux 12.04 USN-3984-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
USN-3984-1

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-May/004902.html

Ubuntu 12.04

linux-image-3.2.0-140-generic_3.2.0-140.186
linux-image-omap_3.2.0.140.155
linux-image-3.2.0-140-virtual_3.2.0-140.186
linux-image-3.2.0-140-highbank_3.2.0-140.186
linux-image-3.2.0-140-generic-pae_3.2.0-140.186
linux-image-powerpc64-smp_3.2.0.140.155
linux-image-virtual_3.2.0.140.155
linux-image-generic-pae_3.2.0.140.155
linux-image-powerpc-smp_3.2.0.140.155
linux-image-powerpc_3.2.0.140.155
linux-image-3.2.0-140-omap_3.2.0-140.186
linux-image-3.2.0-140-powerpc-smp_3.2.0-140.186
linux-image-highbank_3.2.0.140.155
linux-image-generic_3.2.0.140.155
linux-image-3.2.0-140-powerpc64-smp_3.2.0-140.186

186689 - Ubuntu Linux 18.04, 18.10 USN-3973-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6470

Description

The scan detected that the host is missing the following update:
USN-3973-1

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-May/004887.html

Ubuntu 18.10

isc-dhcp-server_4.3.5-3ubuntu9.1

Ubuntu 18.04

isc-dhcp-server_4.3.5-3ubuntu7.1

186694 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3970-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3839

Description

The scan detected that the host is missing the following update:
USN-3970-1

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-May/004882.html

Ubuntu 16.04

ghostscript_9.26~dfsg+0-0ubuntu0.16.04.9
libgs9_9.26~dfsg+0-0ubuntu0.16.04.9

Ubuntu 18.10

libgs9_9.26~dfsg+0-0ubuntu0.18.10.9
ghostscript_9.26~dfsg+0-0ubuntu0.18.10.9

Ubuntu 19.04

ghostscript_9.26~dfsg+0-0ubuntu7.1
libgs9_9.26~dfsg+0-0ubuntu7.1

Ubuntu 18.04

libgs9_9.26~dfsg+0-0ubuntu0.18.04.9
ghostscript_9.26~dfsg+0-0ubuntu0.18.04.9

186695 - Ubuntu Linux 14.04 USN-3983-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
USN-3983-1

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-May/004899.html

Ubuntu 14.04

linux-image-3.13.0-170-powerpc-smp_3.13.0-170.220
linux-image-powerpc-e500mc_3.13.0.170.181
linux-image-generic-lpae_3.13.0.170.181
linux-image-virtual_3.13.0.170.181
linux-image-lowlatency_3.13.0.170.181
linux-image-3.13.0-170-powerpc-e500_3.13.0-170.220
linux-image-powerpc64-smp_3.13.0.170.181

linux-image-3.13.0-170-generic_3.13.0-170.220
linux-image-powerpc64-emb_3.13.0.170.181
linux-image-powerpc-e500_3.13.0.170.181
linux-image-3.13.0-170-powerpc-e500mc_3.13.0-170.220
linux-image-3.13.0-170-lowlatency_3.13.0-170.220
linux-image-3.13.0-170-powerpc64-emb_3.13.0-170.220
linux-image-3.13.0-170-powerpc64-smp_3.13.0-170.220
linux-image-powerpc-smp_3.13.0.170.181
linux-image-generic_3.13.0.170.181
linux-image-3.13.0-170-generic-lpae_3.13.0-170.220

186696 - Ubuntu Linux 12.04 USN-3983-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
USN-3983-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-May/004904.html

Ubuntu 12.04

linux-image-3.13.0-170-generic_3.13.0-170.220~12.04.2+signed1
linux-image-3.13.0-170-lowlatency_3.13.0-170.220~12.04.2+signed1
linux-image-generic-lpae-lts-trusty_3.13.0.170.158
linux-image-generic-lts-trusty_3.13.0.170.158
linux-image-3.13.0-170-generic-lpae_3.13.0-170.220~12.04.2

186704 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3972-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-10129, CVE-2019-10130

Description

The scan detected that the host is missing the following update:
USN-3972-1

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-May/004886.html

Ubuntu 16.04

postgresql-9.5_9.5.17-0ubuntu0.16.04.1

Ubuntu 18.10

postgresql-10_10.8-0ubuntu0.18.10.1

Ubuntu 19.04

postgresql-11_11.3-0ubuntu0.19.04.1

Ubuntu 18.04

postgresql-10_10.8-0ubuntu0.18.04.1

186705 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10, 19.04 USN-3977-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Description

The scan detected that the host is missing the following update:
USN-3977-1

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-May/004892.html

Ubuntu 16.04

intel-microcode_3.20190514.0ubuntu0.16.04.1

Ubuntu 18.10

intel-microcode_3.20190514.0ubuntu0.18.10.1

Ubuntu 19.04

intel-microcode_3.20190514.0ubuntu0.19.04.1

Ubuntu 14.04

intel-microcode_3.20190514.0ubuntu0.14.04.1

Ubuntu 18.04

intel-microcode_3.20190514.0ubuntu0.18.04.2

195151 - Fedora Linux 28 FEDORA-2019-e2d5de3342 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-e2d5de3342

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/2019/5/?count=200&page=2

Fedora Core 28

libqb-1.0.5-1.fc28

195158 - Fedora Linux 28 FEDORA-2019-ca4ee3510d 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-ca4ee3510d

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/2019/5/?count=200&page=2

Fedora Core 28

java-11-openjdk-11.0.3.7-1.fc28

195160 - Fedora Linux 29 FEDORA-2019-265e0b1282 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-2019-265e0b1282

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/2019/5/?count=200&page=2

Fedora Core 29

java-11-openjdk-11.0.3.7-1.fc29

195161 - Fedora Linux 30 FEDORA-2019-b8ae9d5699 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-b8ae9d5699

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/2019/5/?count=200&page=3

Fedora Core 30

exiv2-0.27.1-1.fc30

195162 - Fedora Linux 30 FEDORA-2019-6350c4e21a 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-2019-6350c4e21a

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/2019/5/?count=200&page=2

Fedora Core 30

php-7.3.5-1.fc30

195165 - Fedora Linux 30 FEDORA-2019-cc896df591 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-cc896df591

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/2019/5/?count=200&page=3

Fedora Core 30

mosquitto-1.6.2-1.fc30

195170 - Fedora Linux 29 FEDORA-2019-fb2c321d46 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-fb2c321d46

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/2019/5/?count=200&page=4

Fedora Core 29

perl-YAML-1.28-1.fc29

195172 - Fedora Linux 28 FEDORA-2019-feac6674b7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Description

The scan detected that the host is missing the following update:
FEDORA-2019-feac6674b7

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/2019/5/?count=200&page=3

Fedora Core 28

ruby-2.5.5-108.fc28

147917 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:1238-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-20815, CVE-2019-11091, CVE-2019-3812, CVE-2019-8934, CVE-2019-9824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1238-1

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-May/005453.html

SuSE SLED 12 SP4
x86_64
qemu-debugsource-2.11.2-5.13.1
qemu-kvm-2.11.2-5.13.1
qemu-block-curl-2.11.2-5.13.1
qemu-2.11.2-5.13.1
qemu-x86-2.11.2-5.13.1
qemu-tools-2.11.2-5.13.1
qemu-tools-debuginfo-2.11.2-5.13.1
qemu-block-curl-debuginfo-2.11.2-5.13.1

noarch
qemu-sgabios-8-5.13.1
qemu-seabios-1.11.0-5.13.1
qemu-vgabios-1.11.0-5.13.1
qemu-ipxe-1.0.0+-5.13.1

SuSE SLES 12 SP4
noarch
qemu-sgabios-8-5.13.1
qemu-seabios-1.11.0-5.13.1
qemu-vgabios-1.11.0-5.13.1
qemu-ipxe-1.0.0+-5.13.1

x86_64
qemu-block-rbd-2.11.2-5.13.1
qemu-kvm-2.11.2-5.13.1
qemu-tools-debuginfo-2.11.2-5.13.1
qemu-lang-2.11.2-5.13.1
qemu-guest-agent-debuginfo-2.11.2-5.13.1
qemu-block-ssh-debuginfo-2.11.2-5.13.1
qemu-block-ssh-2.11.2-5.13.1
qemu-guest-agent-2.11.2-5.13.1
qemu-2.11.2-5.13.1
qemu-block-iscsi-debuginfo-2.11.2-5.13.1
qemu-block-iscsi-2.11.2-5.13.1
qemu-x86-2.11.2-5.13.1
qemu-block-curl-2.11.2-5.13.1
qemu-block-curl-debuginfo-2.11.2-5.13.1
qemu-debugsource-2.11.2-5.13.1
qemu-tools-2.11.2-5.13.1
qemu-block-rbd-debuginfo-2.11.2-5.13.1

147919 - SuSE Linux 15.0 openSUSE-SU-2019:1352-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0161

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1352-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-05/msg00051.html

SuSE Linux 15.0
i586
ovmf-2017+git1510945757.b2662641d5-lp150.4.19.1
ovmf-tools-2017+git1510945757.b2662641d5-lp150.4.19.1

noarch
qemu-ovmf-ia32-2017+git1510945757.b2662641d5-lp150.4.19.1
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-lp150.4.19.1

x86_64
ovmf-tools-2017+git1510945757.b2662641d5-lp150.4.19.1
ovmf-2017+git1510945757.b2662641d5-lp150.4.19.1
qemu-ovmf-x86_64-debug-2017+git1510945757.b2662641d5-lp150.4.19.1

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.

182971 - FreeBSD Dovecot Multiple Vulnerabilities (3f98ccb3-6b8a-11e9-9b5c-a4badb296695)

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

Risk Level: Medium

CVE: CVE-2019-11494, CVE-2019-11499

Update Details

Risk is updated

186673 - Ubuntu Linux 18.10, 19.04 USN-3961-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11494, CVE-2019-11499

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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