2019-MAR-13
FSL version 7.6.100

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

194868 - Fedora Linux 28 FEDORA-2019-2dab60e288 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15686, CVE-2018-15687, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2018-16866, CVE-2019-6454

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2dab60e288

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/2019/3/?count=200&page=2

Fedora Core 28

systemd-238-12.git07f8cd5.fc28

194879 - Fedora Linux 28 FEDORA-2019-196ab64d65 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16880, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9162, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
FEDORA-2019-196ab64d65

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/2019/3/?count=200&page=1

Fedora Core 28

kernel-headers-4.20.14-100.fc28
kernel-4.20.14-100.fc28

147699 - SuSE Linux 15.0 openSUSE-SU-2019:0295-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0295-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00026.html

SuSE Linux 15.0
x86_64
docker-18.09.1_ce-lp150.5.13.1
runc-debuginfo-1.0.0~rc6-lp150.2.7.1
containerd-ctr-1.2.2-lp150.4.10.1
docker-runc-debuginfo-1.0.0rc6+gitr3748_96ec2177ae84-lp150.5.14.1
containerd-1.2.2-lp150.4.10.1
docker-libnetwork-0.7.0.1+gitr2711_2cfbf9b1f981-lp150.3.10.1
runc-1.0.0~rc6-lp150.2.7.1
docker-debuginfo-18.09.1_ce-lp150.5.13.1
golang-github-docker-libnetwork-0.7.0.1+gitr2711_2cfbf9b1f981-lp150.3.10.1
docker-test-18.09.1_ce-lp150.5.13.1
docker-debugsource-18.09.1_ce-lp150.5.13.1
docker-test-debuginfo-18.09.1_ce-lp150.5.13.1
docker-libnetwork-debuginfo-0.7.0.1+gitr2711_2cfbf9b1f981-lp150.3.10.1
docker-runc-1.0.0rc6+gitr3748_96ec2177ae84-lp150.5.14.1

noarch
containerd-test-1.2.2-lp150.4.10.1
docker-runc-test-1.0.0rc6+gitr3748_96ec2177ae84-lp150.5.14.1
docker-bash-completion-18.09.1_ce-lp150.5.13.1
docker-zsh-completion-18.09.1_ce-lp150.5.13.1
runc-test-1.0.0~rc6-lp150.2.7.1

24805 - (MSPT-Mar2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0779)

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

Risk Level: High

CVE: CVE-2019-0779

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 the 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.

24807 - (MSPT-Mar2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0592)

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

Risk Level: High

CVE: CVE-2019-0592

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.

24808 - (MSPT-Mar2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0611)

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

Risk Level: High

CVE: CVE-2019-0611

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.

24809 - (MSPT-Mar2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0771)

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

Risk Level: High

CVE: CVE-2019-0771

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 the 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.

24810 - (MSPT-Mar2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0770)

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

Risk Level: High

CVE: CVE-2019-0770

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 the 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.

24811 - (MSPT-Mar2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0769)

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

Risk Level: High

CVE: CVE-2019-0769

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 the 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.

24812 - (MSPT-Mar2019) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0639)

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

Risk Level: High

CVE: CVE-2019-0639

Description

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

Observation

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

The flaw lies in the Improperly Handles Objects in Memory 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.

24813 - (MSPT-Mar2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0773)

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

Risk Level: High

CVE: CVE-2019-0773

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 the 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.

24815 - (MSPT-Mar2019) Microsoft Windows Subsystem for Linux Elevation of Privilege Vulnerability (CVE-2019-0682)

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

Risk Level: High

CVE: CVE-2019-0682

Description

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

Observation

A vulnerability in some versions of Windows Subsystem for Linux could lead to privilege escalation.

The flaw is due to an integer overflow in Windows Subsystem for Linux. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24816 - (MSPT-Mar2019) Microsoft Windows Subsystem for Linux Elevation of Privilege Vulnerability (CVE-2019-0689)

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

Risk Level: High

CVE: CVE-2019-0689

Description

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

Observation

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

The flaw is due to an integer overflow in Windows Subsystem for Linux. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24817 - (MSPT-Mar2019) Microsoft Windows Subsystem for Linux Elevation of Privilege Vulnerability (CVE-2019-0692)

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

Risk Level: High

CVE: CVE-2019-0692

Description

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

Observation

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

The flaw is due to an integer overflow in Windows Subsystem for Linux. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24818 - (MSPT-Mar2019) Microsoft Windows Subsystem for Linux Elevation of Privilege Vulnerability (CVE-2019-0693)

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

Risk Level: High

CVE: CVE-2019-0693

Description

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

Observation

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

The flaw is due to an integer overflow in Windows Subsystem for Linux. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24819 - (MSPT-Mar2019) Microsoft Windows Subsystem for Linux Elevation of Privilege Vulnerability (CVE-2019-0694)

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

Risk Level: High

CVE: CVE-2019-0694

Description

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

Observation

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

The flaw is due to an integer overflow in Windows Subsystem for Linux. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24823 - (MSPT-Mar2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0617)

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

Risk Level: High

CVE: CVE-2019-0617

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 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.

24829 - (MSPT-Mar2019) Microsoft Win32k Elevation of Privilege Vulnerability (CVE-2019-0797)

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

Risk Level: High

CVE: CVE-2019-0797

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 is due to improper handling of objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24830 - (MSPT-Mar2019) Microsoft Win32k Elevation of Privilege Vulnerability (CVE-2019-0808)

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

Risk Level: High

CVE: CVE-2019-0808

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 is due to improper handling of objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24831 - (MSPT-Mar2019) Microsoft Windows Improperly Handles Objects in Memory Denial of Service (CVE-2019-0754)

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

Risk Level: High

CVE: CVE-2019-0754

Description

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

Observation

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

The flaw lies due the improperly handles objects in 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.

24832 - (MSPT-Mar2019) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0772)

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

Risk Level: High

CVE: CVE-2019-0772

Description

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

Observation

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

The flaw lies due to the 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.

24833 - (MSPT-Mar2019) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0784)

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

Risk Level: High

CVE: CVE-2019-0784

Description

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

Observation

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

The flaw lies due to the 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.

24834 - (MSPT-Mar2019) Microsoft Windows TFTP Remote Code Execution (CVE-2019-0603)

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

Risk Level: High

CVE: CVE-2019-0603

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 TFTP 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.

24843 - (MSPT-Mar2019) Microsoft Visual Studio C++ Improperly Validates Input Remote Code Execution (CVE-2019-0809)

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

Risk Level: High

CVE: CVE-2019-0809

Description

A vulnerability in some versions of Microsoft Visual Studio C++ could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Visual Studio C++ could lead to remote code execution.

The flaw lies in the Improperly Validates Input 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.

24845 - (MSPT-Mar2019) Microsoft Windows VBScript Engine Remote Code Execution (CVE-2019-0666)

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

Risk Level: High

CVE: CVE-2019-0666

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 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.

24849 - (MSPT-Mar2019) Microsoft Browser Memory Corruption Vulnerabilty (CVE-2019-0780)

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

Risk Level: High

CVE: CVE-2019-0780

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 due the improper access of 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.

24850 - (MSPT-Mar2019) Microsoft Windows VBScript Engine Remote Code Execution Vulnerability (CVE-2019-0665)

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

Risk Level: High

CVE: CVE-2019-0665

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 in the VBScript 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.

24851 - (MSPT-Mar2019) Microsoft Windows VBScript Engine Remote Code Execution (CVE-2019-0667)

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

Risk Level: High

CVE: CVE-2019-0667

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 in the VBScript 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.

24852 - (MSPT-Mar2019) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2019-0680)

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

Risk Level: High

CVE: CVE-2019-0680

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 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.

24853 - (MSPT-Mar2019) Microsoft Internet Explorer Remote Code Execution Vulnerability (CVE-2019-0763)

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

Risk Level: High

CVE: CVE-2019-0763

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 the improper handling of 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.

24855 - (MSPT-Mar2019) Microsoft Internet Explorer Remote Code Execution Vulnerability (CVE-2019-0783)

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

Risk Level: High

CVE: CVE-2019-0783

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 the improper handling of 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.

24857 - (MSPT-Mar2019) Microsoft Windows Comctl32 Remote Code Execution Vulnerability (CVE-2019-0765)

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

Risk Level: High

CVE: CVE-2019-0765

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 is due to improper handling of 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.

24863 - (MSPT-Mar2019) Microsoft Hyper-V Improperly Validate Input Denial of Service (CVE-2019-0701)

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

Risk Level: High

CVE: CVE-2019-0701

Description

A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service.

The flaw lies in the Improperly Validate Input component. 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.

24864 - (MSPT-Mar2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-0690)

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

Risk Level: High

CVE: CVE-2019-0690

Description

A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service.

The flaw lies in the Network Switch component. 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.

24865 - (MSPT-Mar2019) Microsoft Hyper-V Improperly Validate Input Denial of Service (CVE-2019-0695)

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

Risk Level: High

CVE: CVE-2019-0695

Description

A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service.

The flaw lies in the Improperly Validate Input component. 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.

24867 - (MSPT-Mar2019) Microsoft Office Access Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0748)

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

Risk Level: High

CVE: CVE-2019-0748

Description

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

Observation

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

The flaw lies due the 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.

24868 - (MSPT-Mar2019) Microsoft Windows DHCP Remote Code Execution (CVE-2019-0726)

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

Risk Level: High

CVE: CVE-2019-0726

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.

24869 - (MSPT-Mar2019) Microsoft Windows DHCP Remote Code Execution (CVE-2019-0698)

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

Risk Level: High

CVE: CVE-2019-0698

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. The exploit requires the attacker to have valid credentials to the vulnerable system.

24870 - (MSPT-Mar2019) Microsoft Windows DHCP Remote Code Execution (CVE-2019-0697)

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

Risk Level: High

CVE: CVE-2019-0697

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. The exploit requires the attacker to have valid credentials to the vulnerable system.

24871 - (MSPT-Mar2019) Microsoft MSXML Parser Processes User Input Remote Code Execution (CVE-2019-0756)

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

Risk Level: High

CVE: CVE-2019-0756

Description

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

Observation

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

The flaw lies in the parser processes user input. 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.

24872 - (MSPT-Mar2019) Microsoft SharePoint Server Improperly Sanitize Web Request Remote Code Execution (CVE-

2019-0778)

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

Risk Level: High

CVE: CVE-2019-0778

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 due the improperly sanitize web request. 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.

24875 - (MSPT-Mar2019) Microsoft Windows SMB Information Disclosure (CVE-2019-0821)

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

Risk Level: High

CVE: CVE-2019-0821

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 SMB Server 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.

131308 - Debian Linux 9.0 DSA-4405-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17480, CVE-2018-14423, CVE-2018-18088, CVE-2018-5785, CVE-2018-6616

Description

The scan detected that the host is missing the following update:
DSA-4405-1

Observation

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

http://www.debian.org/security/2019/dsa-4405

Debian 9.0
all
libopenjp2-7-dbg_2.1.2-1.1+deb9u3
libopenjpip-viewer_2.1.2-1.1+deb9u3
libopenjpip7_2.1.2-1.1+deb9u3
libopenjp2-7-dev_2.1.2-1.1+deb9u3

libopenjpip-dec-server_2.1.2-1.1+deb9u3
libopenjpip-server_2.1.2-1.1+deb9u3
libopenjp3d-tools_2.1.2-1.1+deb9u3
libopenjp2-7_2.1.2-1.1+deb9u3
libopenjp3d7_2.1.2-1.1+deb9u3
libopenjp2-tools_2.1.2-1.1+deb9u3

131309 - Debian Linux 9.0 DSA-4403-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9637, CVE-2019-9638, CVE-2019-9639, CVE-2019-9640, CVE-2019-9641, CVE-2019-9675

Description

The scan detected that the host is missing the following update:
DSA-4403-1

Observation

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

http://www.debian.org/security/2019/dsa-4403

Debian 9.0
all
php7.0_7.0.33-0+deb9u3

147695 - SuSE Linux 15.0 openSUSE-SU-2019:0323-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3817

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0323-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00054.html

SuSE Linux 15.0
x86_64
python3-libcomps-0.1.8-lp150.2.3.1
libcomps0_1_6-0.1.8-lp150.2.3.1
python3-libcomps-debuginfo-0.1.8-lp150.2.3.1
libcomps-devel-0.1.8-lp150.2.3.1
python2-libcomps-0.1.8-lp150.2.3.1
libcomps0_1_6-debuginfo-0.1.8-lp150.2.3.1
libcomps-debugsource-0.1.8-lp150.2.3.1
libcomps-debuginfo-0.1.8-lp150.2.3.1
python2-libcomps-debuginfo-0.1.8-lp150.2.3.1

noarch

libcomps-doc-0.1.8-lp150.2.3.1
python-libcomps-doc-0.1.8-lp150.2.3.1

147696 - SuSE Linux 15.0 openSUSE-SU-2019:0297-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1238

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0297-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00025.html

SuSE Linux 15.0
x86_64
amavisd-new-debugsource-2.11.1-lp150.5.3.1
amavisd-new-debuginfo-2.11.1-lp150.5.3.1
amavisd-new-docs-2.11.1-lp150.5.3.1
amavisd-new-2.11.1-lp150.5.3.1

147704 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0581-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0581-1

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-March/005183.html

SuSE SLED 12 SP4
noarch
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-3.8.3

SuSE SLES 12 SP4
noarch
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-3.8.3
qemu-uefi-aarch64-2017+git1510945757.b2662641d5-3.8.3

x86_64
ovmf-2017+git1510945757.b2662641d5-3.8.3
ovmf-tools-2017+git1510945757.b2662641d5-3.8.3

147706 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0298-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5786

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0298-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00029.html

SuSE Linux 15.0
x86_64
chromedriver-debuginfo-72.0.3626.121-lp150.2.46.1
chromium-debugsource-72.0.3626.121-lp150.2.46.1
chromium-72.0.3626.121-lp150.2.46.1
chromedriver-72.0.3626.121-lp150.2.46.1
chromium-debuginfo-72.0.3626.121-lp150.2.46.1

SuSE Linux 42.3
x86_64
chromium-debuginfo-72.0.3626.121-202.1
chromedriver-debuginfo-72.0.3626.121-202.1
chromedriver-72.0.3626.121-202.1
chromium-72.0.3626.121-202.1
chromium-debugsource-72.0.3626.121-202.1

147710 - SuSE SLES 12 SP3 SUSE-SU-2019:0579-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0579-1

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-March/005181.html

SuSE SLES 12 SP3
noarch
qemu-ovmf-x86_64-2017+git1492060560.b6d11d7c46-4.20.1
qemu-uefi-aarch64-2017+git1492060560.b6d11d7c46-4.20.1

x86_64
ovmf-tools-2017+git1492060560.b6d11d7c46-4.20.1
ovmf-2017+git1492060560.b6d11d7c46-4.20.1

163818 - Oracle Enterprise Linux ELSA-2019-4575 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17807, CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-16862, CVE-2018-18559, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
ELSA-2019-4575

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008523.html
http://oss.oracle.com/pipermail/el-errata/2019-March/008522.html

OEL7
x86_64
kernel-uek-devel-4.1.12-124.26.1.el7uek
kernel-uek-firmware-4.1.12-124.26.1.el7uek
kernel-uek-4.1.12-124.26.1.el7uek
kernel-uek-debug-4.1.12-124.26.1.el7uek
kernel-uek-debug-devel-4.1.12-124.26.1.el7uek
kernel-uek-doc-4.1.12-124.26.1.el7uek

OEL6
x86_64
kernel-uek-debug-4.1.12-124.26.1.el6uek
kernel-uek-doc-4.1.12-124.26.1.el6uek
kernel-uek-debug-devel-4.1.12-124.26.1.el6uek
kernel-uek-devel-4.1.12-124.26.1.el6uek
kernel-uek-firmware-4.1.12-124.26.1.el6uek
kernel-uek-4.1.12-124.26.1.el6uek

163819 - Oracle Enterprise Linux ELSA-2019-4576 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17807, CVE-2018-10876, CVE-2018-10878, CVE-2018-13053, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
ELSA-2019-4576

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008521.html
http://oss.oracle.com/pipermail/el-errata/2019-March/008520.html

OEL7
x86_64
kernel-uek-3.8.13-118.31.1.el7uek

kernel-uek-firmware-3.8.13-118.31.1.el7uek
kernel-uek-doc-3.8.13-118.31.1.el7uek
dtrace-modules-3.8.13-118.31.1.el7uek-0.4.5-3.el7
kernel-uek-debug-devel-3.8.13-118.31.1.el7uek
kernel-uek-debug-3.8.13-118.31.1.el7uek
kernel-uek-devel-3.8.13-118.31.1.el7uek

OEL6
x86_64
dtrace-modules-3.8.13-118.31.1.el6uek-0.4.5-3.el6
kernel-uek-debug-3.8.13-118.31.1.el6uek
kernel-uek-firmware-3.8.13-118.31.1.el6uek
kernel-uek-devel-3.8.13-118.31.1.el6uek
kernel-uek-3.8.13-118.31.1.el6uek
kernel-uek-debug-devel-3.8.13-118.31.1.el6uek
kernel-uek-doc-3.8.13-118.31.1.el6uek

163820 - Oracle Enterprise Linux ELSA-2019-4577 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10876, CVE-2018-13053, CVE-2018-17972, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
ELSA-2019-4577

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008524.html

OEL6
x86_64
kernel-uek-doc-2.6.39-400.307.1.el6uek
kernel-uek-debug-devel-2.6.39-400.307.1.el6uek
kernel-uek-devel-2.6.39-400.307.1.el6uek
kernel-uek-firmware-2.6.39-400.307.1.el6uek
kernel-uek-debug-2.6.39-400.307.1.el6uek
kernel-uek-2.6.39-400.307.1.el6uek

i386
kernel-uek-doc-2.6.39-400.307.1.el6uek
kernel-uek-debug-devel-2.6.39-400.307.1.el6uek
kernel-uek-devel-2.6.39-400.307.1.el6uek
kernel-uek-firmware-2.6.39-400.307.1.el6uek
kernel-uek-debug-2.6.39-400.307.1.el6uek
kernel-uek-2.6.39-400.307.1.el6uek

163822 - Oracle Enterprise Linux ELSA-2019-4570 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000026, CVE-2018-14609, CVE-2018-14612, CVE-2018-16862

Description

The scan detected that the host is missing the following update:
ELSA-2019-4570

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008527.html

OEL7
x86_64
kernel-uek-4.14.35-1844.3.2.el7uek
kernel-uek-debug-4.14.35-1844.3.2.el7uek
kernel-uek-debug-devel-4.14.35-1844.3.2.el7uek
kernel-uek-tools-4.14.35-1844.3.2.el7uek
kernel-uek-devel-4.14.35-1844.3.2.el7uek
kernel-uek-doc-4.14.35-1844.3.2.el7uek

171072 - Amazon Linux AMI ALAS-2019-1167 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8912

Description

The scan detected that the host is missing the following update:
ALAS-2019-1167

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1167.html

Amazon Linux AMI
x86_64
kernel-devel-4.14.104-78.84.amzn1
kernel-tools-devel-4.14.104-78.84.amzn1
kernel-debuginfo-common-x86_64-4.14.104-78.84.amzn1
perf-debuginfo-4.14.104-78.84.amzn1
perf-4.14.104-78.84.amzn1
kernel-4.14.104-78.84.amzn1
kernel-debuginfo-4.14.104-78.84.amzn1
kernel-tools-4.14.104-78.84.amzn1
kernel-tools-debuginfo-4.14.104-78.84.amzn1
kernel-headers-4.14.104-78.84.amzn1

i686
kernel-devel-4.14.104-78.84.amzn1
kernel-tools-devel-4.14.104-78.84.amzn1
kernel-tools-4.14.104-78.84.amzn1
perf-debuginfo-4.14.104-78.84.amzn1
perf-4.14.104-78.84.amzn1
kernel-4.14.104-78.84.amzn1
kernel-debuginfo-4.14.104-78.84.amzn1
kernel-tools-debuginfo-4.14.104-78.84.amzn1
kernel-debuginfo-common-i686-4.14.104-78.84.amzn1

kernel-headers-4.14.104-78.84.amzn1

182930 - FreeBSD Rssh - Multiple Vulnerabilities (d193aa9f-3f8c-11e9-9a24-6805ca0b38e8)

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

Risk Level: High

CVE: CVE-2019-1000018, CVE-2019-3463, CVE-2019-3464

Description

The scan detected that the host is missing the following update:
rssh - multiple vulnerabilities (d193aa9f-3f8c-11e9-9a24-6805ca0b38e8)

Observation

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

http://www.vuxml.org/freebsd/d193aa9f-3f8c-11e9-9a24-6805ca0b38e8.html

Affected packages:
rssh < 2.3.4_2

186605 - Ubuntu Linux 14.04, 16.04 USN-3902-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024

Description

The scan detected that the host is missing the following update:
USN-3902-1

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-March/004791.html

Ubuntu 14.04

php5-xmlrpc_5.5.9+dfsg-1ubuntu4.27
php5-fpm_5.5.9+dfsg-1ubuntu4.27
php5-cli_5.5.9+dfsg-1ubuntu4.27
php5-cgi_5.5.9+dfsg-1ubuntu4.27
libapache2-mod-php5_5.5.9+dfsg-1ubuntu4.27

Ubuntu 16.04

php7.0-fpm_7.0.33-0ubuntu0.16.04.2
php7.0-cli_7.0.33-0ubuntu0.16.04.2
php7.0-mbstring_7.0.33-0ubuntu0.16.04.2
php7.0-cgi_7.0.33-0ubuntu0.16.04.2
php7.0-xmlrpc_7.0.33-0ubuntu0.16.04.2
libapache2-mod-php7.0_7.0.33-0ubuntu0.16.04.2

194853 - Fedora Linux 28 FEDORA-2019-d248c5aa39 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000480, CVE-2018-13982, CVE-2018-16831

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d248c5aa39

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/2019/3/?count=200&page=2

Fedora Core 28

php-Smarty-3.1.33-1.fc28

194858 - Fedora Linux 28 FEDORA-2019-82df33e428 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-82df33e428

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/2019/3/?count=200&page=2

Fedora Core 28

drupal7-7.64-1.fc28

194869 - Fedora Linux 29 FEDORA-2019-87e7046631 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16862, CVE-2018-16880, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
FEDORA-2019-87e7046631

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/2019/3/?count=200&page=1

Fedora Core 29

kernel-4.20.14-200.fc29
kernel-headers-4.20.14-200.fc29

194873 - Fedora Linux 29 FEDORA-2019-e595e8a7d7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000480, CVE-2018-13982, CVE-2018-16831

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e595e8a7d7

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

Fedora Core 29

php-Smarty-3.1.33-1.fc29

194877 - Fedora Linux 29 FEDORA-2019-3e89502cb1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18883, CVE-2018-19961, CVE-2018-19962, CVE-2018-19963, CVE-2018-19964, CVE-2018-19965, CVE-2018-19966, CVE-2018-19967

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3e89502cb1

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/2019/3/?count=200&page=1

Fedora Core 29

xen-4.11.1-4.fc29

194878 - Fedora Linux 28 FEDORA-2019-6a0717dc9a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6930, CVE-2017-6931, CVE-2018-7600, CVE-2018-7602, CVE-2018-9861

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6a0717dc9a

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/2019/3/?count=200&page=2

Fedora Core 28

php-typo3-phar-stream-wrapper2-2.0.1-1.fc28
drupal8-8.6.10-1.fc28

196264 - Red Hat Enterprise Linux RHSA-2019-0469 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11212, CVE-2018-12547, CVE-2018-12549, CVE-2019-2422, CVE-2019-2449

Description

The scan detected that the host is missing the following update:
RHSA-2019-0469

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00009.html

RHEL6D
x86_64
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el6_10

i386
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el6_10

RHEL6S
i386
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el6_10

x86_64

java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el6_10

RHEL6WS
x86_64
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el6_10

i386
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el6_10
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el6_10

196265 - Red Hat Enterprise Linux RHSA-2019-0474 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11212, CVE-2018-12547, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0474

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00012.html

RHEL6D
x86_64
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el6_10

i386
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el6_10

RHEL6S

i386
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el6_10

x86_64
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el6_10

RHEL6WS
x86_64
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el6_10

i386
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el6_10

196266 - Red Hat Enterprise Linux RHSA-2019-0481 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5786

Description

The scan detected that the host is missing the following update:
RHSA-2019-0481

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00013.html

RHEL6D
i386
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

i686
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

x86_64
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

RHEL6S
i386
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

i686
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

x86_64
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

RHEL6WS
i386
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

i686
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

x86_64
chromium-browser-debuginfo-72.0.3626.121-1.el6_10
chromium-browser-72.0.3626.121-1.el6_10

196267 - Red Hat Enterprise Linux RHSA-2019-0473 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11212, CVE-2018-12547, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0473

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00011.html

RHEL7D
x86_64
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el7

RHEL7S
x86_64
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el7

java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el7

RHEL7WS
x86_64
java-1.7.1-ibm-src-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-demo-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-devel-1.7.1.4.40-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.4.40-1jpp.1.el7

196268 - Red Hat Enterprise Linux RHSA-2019-0472 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11212, CVE-2018-12547, CVE-2018-12549, CVE-2019-2422, CVE-2019-2449

Description

The scan detected that the host is missing the following update:
RHSA-2019-0472

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00010.html

RHEL7D
x86_64
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el7

RHEL7S
x86_64
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el7

RHEL7WS
x86_64
java-1.8.0-ibm-src-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-plugin-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-demo-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-devel-1.8.0.5.30-1jpp.1.el7
java-1.8.0-ibm-jdbc-1.8.0.5.30-1jpp.1.el7

147700 - SuSE Linux 15.0 openSUSE-SU-2019:0308-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464, CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0308-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00037.html

SuSE Linux 15.0
i586
webkit2gtk3-debugsource-2.22.6-lp150.2.12.1
webkit2gtk-4_0-injected-bundles-2.22.6-lp150.2.12.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.6-lp150.2.12.1
typelib-1_0-WebKit2-4_0-2.22.6-lp150.2.12.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-lp150.2.12.1
webkit2gtk3-minibrowser-2.22.6-lp150.2.12.1
webkit-jsc-4-2.22.6-lp150.2.12.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-lp150.2.12.1
webkit-jsc-4-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-minibrowser-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-devel-2.22.6-lp150.2.12.1
libwebkit2gtk-4_0-37-2.22.6-lp150.2.12.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.6-lp150.2.12.1
webkit2gtk3-plugin-process-gtk2-2.22.6-lp150.2.12.1
libjavascriptcoregtk-4_0-18-2.22.6-lp150.2.12.1

noarch
libwebkit2gtk3-lang-2.22.6-lp150.2.12.1

x86_64
libwebkit2gtk-4_0-37-32bit-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-debugsource-2.22.6-lp150.2.12.1
webkit2gtk-4_0-injected-bundles-2.22.6-lp150.2.12.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.6-lp150.2.12.1
typelib-1_0-WebKit2-4_0-2.22.6-lp150.2.12.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-lp150.2.12.1
libjavascriptcoregtk-4_0-18-32bit-2.22.6-lp150.2.12.1
webkit2gtk3-minibrowser-2.22.6-lp150.2.12.1
webkit-jsc-4-2.22.6-lp150.2.12.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-lp150.2.12.1
libwebkit2gtk-4_0-37-32bit-2.22.6-lp150.2.12.1
webkit-jsc-4-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-minibrowser-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-lp150.2.12.1
webkit2gtk3-devel-2.22.6-lp150.2.12.1
libwebkit2gtk-4_0-37-2.22.6-lp150.2.12.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.6-lp150.2.12.1

webkit2gtk3-plugin-process-gtk2-2.22.6-lp150.2.12.1
libjavascriptcoregtk-4_0-18-2.22.6-lp150.2.12.1
libjavascriptcoregtk-4_0-18-32bit-debuginfo-2.22.6-lp150.2.12.1

147707 - SuSE Linux 15.0 openSUSE-SU-2019:0310-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3825

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0310-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00041.html

SuSE Linux 15.0
x86_64
gdm-debugsource-3.26.2.1-lp150.11.9.1
gdm-debuginfo-3.26.2.1-lp150.11.9.1
libgdm1-debuginfo-3.26.2.1-lp150.11.9.1
typelib-1_0-Gdm-1_0-3.26.2.1-lp150.11.9.1
libgdm1-3.26.2.1-lp150.11.9.1
gdm-3.26.2.1-lp150.11.9.1
gdm-devel-3.26.2.1-lp150.11.9.1

noarch
gdm-branding-upstream-3.26.2.1-lp150.11.9.1
gdm-lang-3.26.2.1-lp150.11.9.1
gdmflexiserver-3.26.2.1-lp150.11.9.1

147708 - SuSE Linux 42.3 openSUSE-SU-2019:0309-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0309-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00038.html

SuSE Linux 42.3
i586
webkit2gtk3-devel-2.22.6-21.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-21.1

libwebkit2gtk-4_0-37-2.22.6-21.1
typelib-1_0-WebKit2-4_0-2.22.6-21.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-21.1
webkit-jsc-4-2.22.6-21.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.6-21.1
webkit-jsc-4-debuginfo-2.22.6-21.1
webkit2gtk3-debugsource-2.22.6-21.1
webkit2gtk3-minibrowser-2.22.6-21.1
webkit2gtk3-plugin-process-gtk2-2.22.6-21.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.6-21.1
libjavascriptcoregtk-4_0-18-2.22.6-21.1
webkit2gtk3-minibrowser-debuginfo-2.22.6-21.1
webkit2gtk-4_0-injected-bundles-2.22.6-21.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-21.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-21.1

noarch
libwebkit2gtk3-lang-2.22.6-21.1

x86_64
webkit2gtk3-devel-2.22.6-21.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-21.1
libwebkit2gtk-4_0-37-2.22.6-21.1
typelib-1_0-WebKit2-4_0-2.22.6-21.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-21.1
webkit-jsc-4-2.22.6-21.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.6-21.1
webkit-jsc-4-debuginfo-2.22.6-21.1
webkit2gtk3-debugsource-2.22.6-21.1
libwebkit2gtk-4_0-37-debuginfo-32bit-2.22.6-21.1
webkit2gtk3-minibrowser-2.22.6-21.1
libwebkit2gtk-4_0-37-32bit-2.22.6-21.1
libjavascriptcoregtk-4_0-18-32bit-2.22.6-21.1
webkit2gtk3-plugin-process-gtk2-2.22.6-21.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.6-21.1
libjavascriptcoregtk-4_0-18-2.22.6-21.1
webkit2gtk3-minibrowser-debuginfo-2.22.6-21.1
libjavascriptcoregtk-4_0-18-debuginfo-32bit-2.22.6-21.1
webkit2gtk-4_0-injected-bundles-2.22.6-21.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-21.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-21.1

171074 - Amazon Linux AMI ALAS-2019-1172 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6486

Description

The scan detected that the host is missing the following update:
ALAS-2019-1172

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1172.html

Amazon Linux AMI
i686
golang-1.10.6-1.48.amzn1
golang-bin-1.10.6-1.48.amzn1

noarch
golang-tests-1.10.6-1.48.amzn1
golang-docs-1.10.6-1.48.amzn1
golang-src-1.10.6-1.48.amzn1
golang-misc-1.10.6-1.48.amzn1

x86_64
golang-race-1.10.6-1.48.amzn1
golang-bin-1.10.6-1.48.amzn1
golang-1.10.6-1.48.amzn1

186597 - Ubuntu Linux 18.10 USN-3903-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16880, CVE-2018-18397, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3903-1

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-March/004792.html

Ubuntu 18.10

linux-image-lowlatency_4.18.0.16.17
linux-image-4.18.0-1007-gcp_4.18.0-1007.8
linux-image-snapdragon_4.18.0.16.17
linux-image-kvm_4.18.0.1008.8
linux-image-generic-lpae_4.18.0.16.17
linux-image-4.18.0-16-generic-lpae_4.18.0-16.17
linux-image-4.18.0-1008-kvm_4.18.0-1008.8
linux-image-4.18.0-16-lowlatency_4.18.0-16.17
linux-image-4.18.0-1010-raspi2_4.18.0-1010.12
linux-image-azure_4.18.0.1013.14
linux-image-generic_4.18.0.16.17
linux-image-gke_4.18.0.1007.7
linux-image-raspi2_4.18.0.1010.7
linux-image-4.18.0-16-generic_4.18.0-16.17
linux-image-gcp_4.18.0.1007.7
linux-image-4.18.0-16-snapdragon_4.18.0-16.17
linux-image-4.18.0-1013-azure_4.18.0-1013.13

186598 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3906-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10779, CVE-2018-12900, CVE-2018-17000, CVE-2018-19210, CVE-2019-6128, CVE-2019-7663

Description

The scan detected that the host is missing the following update:
USN-3906-1

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-March/004796.html

Ubuntu 16.04

libtiff-tools_4.0.6-1ubuntu0.6
libtiff5_4.0.6-1ubuntu0.6

Ubuntu 18.10

libtiff-tools_4.0.9-6ubuntu0.2
libtiff5_4.0.9-6ubuntu0.2

Ubuntu 14.04

libtiff5_4.0.3-7ubuntu0.11
libtiff-tools_4.0.3-7ubuntu0.11

Ubuntu 18.04

libtiff5_4.0.9-5ubuntu0.2
libtiff-tools_4.0.9-5ubuntu0.2

186604 - Ubuntu Linux 18.04 USN-3903-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16880, CVE-2018-18397, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3903-2

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-March/004793.html

Ubuntu 18.04

linux-image-generic-hwe-18.04_4.18.0.16.66
linux-image-4.18.0-1013-azure_4.18.0-1013.13~18.04.1
linux-image-lowlatency-hwe-18.04_4.18.0.16.66
linux-image-4.18.0-16-generic-lpae_4.18.0-16.17~18.04.1
linux-image-4.18.0-16-snapdragon_4.18.0-16.17~18.04.1
linux-image-4.18.0-16-lowlatency_4.18.0-16.17~18.04.1
linux-image-4.18.0-16-generic_4.18.0-16.17~18.04.1
linux-image-azure_4.18.0.1013.12

linux-image-snapdragon-hwe-18.04_4.18.0.16.66
linux-image-generic-lpae-hwe-18.04_4.18.0.16.66

194852 - Fedora Linux 29 FEDORA-2019-e0d49261b9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6358, CVE-2018-7867, CVE-2018-7868, CVE-2018-7870, CVE-2018-7871, CVE-2018-7872, CVE-2018-7875, CVE-2018-9165

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e0d49261b9

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

Fedora Core 29

ming-0.4.9-0.1.20181112git5009802.fc29

194856 - Fedora Linux 29 FEDORA-2019-7d0d59764e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10936

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7d0d59764e

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/2019/3/?count=200&page=1

Fedora Core 29

postgresql-jdbc-42.2.5-2.fc29

194859 - Fedora Linux 28 FEDORA-2019-c90f32a130 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10360, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c90f32a130

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/2019/3/?count=200&page=1

Fedora Core 28

file-5.33-10.fc28

194862 - Fedora Linux 28 FEDORA-2019-4fdf19459d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6358, CVE-2018-7867, CVE-2018-7868, CVE-2018-7870, CVE-2018-7871, CVE-2018-7872, CVE-2018-7875, CVE-2018-9165

Description

The scan detected that the host is missing the following update:
FEDORA-2019-4fdf19459d

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/2019/3/?count=200&page=2

Fedora Core 28

ming-0.4.9-0.1.20181112git5009802.fc28

194870 - Fedora Linux 28 FEDORA-2019-1b9e80874d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10936

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1b9e80874d

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/2019/3/?count=200&page=1

Fedora Core 28

postgresql-jdbc-42.2.5-2.fc28

24392 - (MSPT-Nov2018) Microsoft Windows Exchange Privilege Escalation (CVE-2018-8581)

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

Risk Level: Medium

CVE: CVE-2018-8581

Description

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

Observation

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

The flaw lies in the registry key 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.

24804 - (MSPT-Mar2019) Microsoft Edge Improperly Enforce Cross-Domain Policies Privilege Escalation (CVE-2019-0678)

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

Risk Level: Medium

CVE: CVE-2019-0678

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 Improperly Enforce Cross-Domain Policies 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.

24806 - (MSPT-Mar2019) Microsoft Edge Click2Play Security Bypass (CVE-2019-0612)

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

Risk Level: Medium

CVE: CVE-2019-0612

Description

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

Observation

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

The flaw lies in the Click2Play component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the user to open a vulnerable website, email or document.

24820 - (MSPT-Mar2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0614)

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

Risk Level: Medium

CVE: CVE-2019-0614

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.

24821 - (MSPT-Mar2019) Microsoft Windows Print Spooler Information Disclosure Vulnerability (CVE-2019-0759)

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

Risk Level: Medium

CVE: CVE-2019-0759

Description

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

Observation

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

The flaw is due to improper handling of objects in memory. 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.

24822 - (MSPT-Mar2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0774)

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

Risk Level: Medium

CVE: CVE-2019-0774

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.

24825 - (MSPT-Mar2019) Microsoft Windows SMB Server Information Disclosure (CVE-2019-0703)

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

Risk Level: Medium

CVE: CVE-2019-0703

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 SMB Server 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.

24826 - (MSPT-Mar2019) Microsoft Windows SMB Server Information Disclosure (CVE-2019-0704)

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

Risk Level: Medium

CVE: CVE-2019-0704

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 SMB Server 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.

24827 - (MSPT-Mar2019) Microsoft Windows Internet Security Zone Security Bypass (CVE-2019-0761)

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

Risk Level: Medium

CVE: CVE-2019-0761

Description

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

Observation

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

The flaw lies in the internet security zone component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the user to open a vulnerable website, email or document.

24835 - (MSPT-Mar2019) Microsoft Windows AppX Deployment Server Privilege Escalation (CVE-2019-0766)

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

Risk Level: Medium

CVE: CVE-2019-0766

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 appx deployment server 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.

24836 - (MSPT-Mar2019) Microsoft Kernel Improperly Initialize a Memory Address Information Disclosure (CVE-2019-0782)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2019-0782

Description

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

Observation

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

The flaw lies due to improperly initialize a memory address. 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.

24837 - (MSPT-Mar2019) Microsoft Kernel Improperly Handles Objects in Memory Information Disclosure (CVE-2019-0775)

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

Risk Level: Medium

CVE: CVE-2019-0775

Description

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

Observation

A vulnerability in some versions of Microsoft Kernel 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 attacker to have valid credentials to the vulnerable system.

24838 - (MSPT-Mar2019) Microsoft Kernel Improperly Handles Objects in Memory Information Disclosure (CVE-2019-0702)

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

Risk Level: Medium

CVE: CVE-2019-0702

Description

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

Observation

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

The flaw lies in the Improperly Handles Objects in the Memory 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.

24839 - (MSPT-Mar2019) Microsoft Kernel Improperly Handles Objects in Memory Information Disclosure (CVE-2019-0755)

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

Risk Level: Medium

CVE: CVE-2019-0755

Description

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

Observation

A vulnerability in some versions of Microsoft Kernel 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 attacker to have valid credentials to the vulnerable system.

24840 - (MSPT-Mar2019) Microsoft Kernel Improperly Initializes Objects in Memory Information Disclosure (CVE-2019-0767)

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

Risk Level: Medium

CVE: CVE-2019-0767

Description

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

Observation

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

The flaw lies due to the improperly initializes objects in memory. 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.

24841 - (MSPT-Mar2019) Microsoft Kernel Improperly Handle Objects in Memory Privilege Escalation (CVE-2019-0696)

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

Risk Level: Medium

CVE: CVE-2019-0696

Description

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

Observation

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

The flaw lies in the Improperly Handle Objects in the Memory 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.

24842 - (MSPT-Mar2019) Microsoft win32k Improperly Provides Kernel Information Information Disclosure (CVE-2019-0776)

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

Risk Level: Medium

CVE: CVE-2019-0776

Description

A vulnerability in some versions of Microsoft win32k could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft win32k could lead to information disclosure.

The flaw lies due to the improperly provides kernel information. 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.

24844 - (MSPT-Mar2019) Microsoft Browsers Scripting Engine Remote Code Execution (CVE-2019-0609)

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

Risk Level: Medium

CVE: CVE-2019-0609

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.

24846 - (MSPT-Mar2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0746)

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

Risk Level: Medium

CVE: CVE-2019-0746

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.

24847 - (MSPT-Mar2019) Microsoft Browsers Security Bypass Vulnerability(CVE-2019-0762)

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

Risk Level: Medium

CVE: CVE-2019-0762

Description

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

Observation

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

The flaw is due the improper handling of requests. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the user to open a vulnerable website, email or document.

24854 - (MSPT-Mar2019) Microsoft Internet Explorer VBScript Execution Policy Security Bypass (CVE-2019-0768)

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

Risk Level: Medium

CVE: CVE-2019-0768

Description

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

Observation

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

The flaw is due the vbscript execution policy. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the user to open a vulnerable website, email or document.

24866 - (MSPT-Mar2019) Microsoft Skype for Business and Lync Spoofing Vulnerability (CVE-2019-0798)

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

Risk Level: Medium

CVE: CVE-2019-0798

Description

A vulnerability in some versions of Microsoft Skype for Business Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Skype for Business Server could lead to spoofing.

The flaw lies due the improperly sanitize request. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

24874 - (MSPT-Mar2019) Microsoft Active Directory Forest Privilege Escalation (CVE-2019-0683)

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

Risk Level: Medium

CVE: CVE-2019-0683

Description

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

Observation

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

The flaw lies in the Forest 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.

147694 - SuSE Linux 42.3 openSUSE-SU-2019:0305-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0305-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00031.html

SuSE Linux 42.3
i586
apache2-worker-2.4.23-37.1
apache2-event-2.4.23-37.1
apache2-prefork-2.4.23-37.1
apache2-utils-2.4.23-37.1
apache2-worker-debuginfo-2.4.23-37.1
apache2-devel-2.4.23-37.1
apache2-debuginfo-2.4.23-37.1
apache2-2.4.23-37.1
apache2-example-pages-2.4.23-37.1
apache2-utils-debuginfo-2.4.23-37.1
apache2-prefork-debuginfo-2.4.23-37.1
apache2-event-debuginfo-2.4.23-37.1
apache2-debugsource-2.4.23-37.1

noarch
apache2-doc-2.4.23-37.1

x86_64
apache2-worker-2.4.23-37.1
apache2-event-2.4.23-37.1
apache2-prefork-2.4.23-37.1
apache2-utils-2.4.23-37.1
apache2-worker-debuginfo-2.4.23-37.1
apache2-devel-2.4.23-37.1
apache2-debuginfo-2.4.23-37.1
apache2-2.4.23-37.1
apache2-example-pages-2.4.23-37.1
apache2-utils-debuginfo-2.4.23-37.1
apache2-prefork-debuginfo-2.4.23-37.1
apache2-event-debuginfo-2.4.23-37.1
apache2-debugsource-2.4.23-37.1

147698 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0563-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5186

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0563-1

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-March/005175.html

SuSE SLED 12 SP4
x86_64
libaudit1-32bit-2.8.1-10.3.2
libaudit1-2.8.1-10.3.2
libaudit1-debuginfo-32bit-2.8.1-10.3.2
libauparse0-2.8.1-10.3.2
audit-debugsource-2.8.1-10.3.2
audit-2.8.1-10.3.2
libaudit1-debuginfo-2.8.1-10.3.2
libauparse0-debuginfo-2.8.1-10.3.2
audit-debuginfo-2.8.1-10.3.2
audit-secondary-debugsource-2.8.1-10.3.2

SuSE SLES 12 SP4
x86_64
libauparse0-2.8.1-10.3.2
audit-debuginfo-2.8.1-10.3.2
libaudit1-debuginfo-32bit-2.8.1-10.3.2
libaudit1-32bit-2.8.1-10.3.2
audit-audispd-plugins-2.8.1-10.3.2
audit-debugsource-2.8.1-10.3.2
audit-audispd-plugins-debuginfo-2.8.1-10.3.2
audit-2.8.1-10.3.2
libauparse0-debuginfo-2.8.1-10.3.2
libaudit1-2.8.1-10.3.2
python2-audit-2.8.1-10.3.2
python3-audit-debuginfo-2.8.1-10.3.2
audit-secondary-debugsource-2.8.1-10.3.2
python2-audit-debuginfo-2.8.1-10.3.2
python3-audit-2.8.1-10.3.2
libaudit1-debuginfo-2.8.1-10.3.2

147701 - SuSE Linux 15.0 openSUSE-SU-2019:0296-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0296-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00027.html

SuSE Linux 15.0
i586
apache2-example-pages-2.4.33-lp150.2.9.1
apache2-debugsource-2.4.33-lp150.2.9.1
apache2-devel-2.4.33-lp150.2.9.1
apache2-prefork-debuginfo-2.4.33-lp150.2.9.1
apache2-worker-debuginfo-2.4.33-lp150.2.9.1
apache2-2.4.33-lp150.2.9.1

apache2-utils-2.4.33-lp150.2.9.1
apache2-debuginfo-2.4.33-lp150.2.9.1
apache2-prefork-2.4.33-lp150.2.9.1
apache2-worker-2.4.33-lp150.2.9.1
apache2-utils-debuginfo-2.4.33-lp150.2.9.1
apache2-event-2.4.33-lp150.2.9.1
apache2-event-debuginfo-2.4.33-lp150.2.9.1

noarch
apache2-doc-2.4.33-lp150.2.9.1

x86_64
apache2-example-pages-2.4.33-lp150.2.9.1
apache2-debugsource-2.4.33-lp150.2.9.1
apache2-devel-2.4.33-lp150.2.9.1
apache2-prefork-debuginfo-2.4.33-lp150.2.9.1
apache2-worker-debuginfo-2.4.33-lp150.2.9.1
apache2-2.4.33-lp150.2.9.1
apache2-utils-2.4.33-lp150.2.9.1
apache2-debuginfo-2.4.33-lp150.2.9.1
apache2-prefork-2.4.33-lp150.2.9.1
apache2-worker-2.4.33-lp150.2.9.1
apache2-utils-debuginfo-2.4.33-lp150.2.9.1
apache2-event-2.4.33-lp150.2.9.1
apache2-event-debuginfo-2.4.33-lp150.2.9.1

147702 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0556-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10852, CVE-2019-3811

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0556-1

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-March/005173.html

SuSE SLED 12 SP4
x86_64
sssd-krb5-common-debuginfo-1.16.1-4.3.2
sssd-tools-debuginfo-1.16.1-4.3.2
sssd-debuginfo-1.16.1-4.3.2
sssd-ad-debuginfo-1.16.1-4.3.2
libsss_nss_idmap0-debuginfo-1.16.1-4.3.2
libsss_idmap0-1.16.1-4.3.2
sssd-ad-1.16.1-4.3.2
sssd-proxy-debuginfo-1.16.1-4.3.2
sssd-32bit-1.16.1-4.3.2
sssd-debugsource-1.16.1-4.3.2
sssd-krb5-common-1.16.1-4.3.2
sssd-ipa-1.16.1-4.3.2
libsss_nss_idmap0-1.16.1-4.3.2
sssd-krb5-debuginfo-1.16.1-4.3.2

libipa_hbac0-1.16.1-4.3.2
libsss_idmap0-debuginfo-1.16.1-4.3.2
sssd-ldap-debuginfo-1.16.1-4.3.2
sssd-ldap-1.16.1-4.3.2
libsss_simpleifp0-debuginfo-1.16.1-4.3.2
sssd-tools-1.16.1-4.3.2
sssd-krb5-1.16.1-4.3.2
python-sssd-config-1.16.1-4.3.2
libipa_hbac0-debuginfo-1.16.1-4.3.2
libsss_certmap0-1.16.1-4.3.2
sssd-1.16.1-4.3.2
libsss_simpleifp0-1.16.1-4.3.2
libsss_certmap0-debuginfo-1.16.1-4.3.2
sssd-debuginfo-32bit-1.16.1-4.3.2
python-sssd-config-debuginfo-1.16.1-4.3.2
sssd-ipa-debuginfo-1.16.1-4.3.2
sssd-proxy-1.16.1-4.3.2

SuSE SLES 12 SP4
x86_64
sssd-krb5-common-debuginfo-1.16.1-4.3.2
sssd-tools-debuginfo-1.16.1-4.3.2
sssd-debuginfo-1.16.1-4.3.2
sssd-ad-debuginfo-1.16.1-4.3.2
libsss_nss_idmap0-debuginfo-1.16.1-4.3.2
libsss_idmap0-1.16.1-4.3.2
sssd-ad-1.16.1-4.3.2
sssd-32bit-1.16.1-4.3.2
sssd-debugsource-1.16.1-4.3.2
sssd-krb5-common-1.16.1-4.3.2
sssd-ipa-1.16.1-4.3.2
libsss_nss_idmap0-1.16.1-4.3.2
sssd-krb5-debuginfo-1.16.1-4.3.2
libipa_hbac0-1.16.1-4.3.2
libsss_idmap0-debuginfo-1.16.1-4.3.2
sssd-ldap-debuginfo-1.16.1-4.3.2
sssd-ldap-1.16.1-4.3.2
libsss_simpleifp0-debuginfo-1.16.1-4.3.2
sssd-tools-1.16.1-4.3.2
sssd-krb5-1.16.1-4.3.2
sssd-debuginfo-32bit-1.16.1-4.3.2
python-sssd-config-1.16.1-4.3.2
libipa_hbac0-debuginfo-1.16.1-4.3.2
libsss_certmap0-1.16.1-4.3.2
sssd-1.16.1-4.3.2
libsss_simpleifp0-1.16.1-4.3.2
libsss_certmap0-debuginfo-1.16.1-4.3.2
sssd-proxy-debuginfo-1.16.1-4.3.2
python-sssd-config-debuginfo-1.16.1-4.3.2
sssd-ipa-debuginfo-1.16.1-4.3.2
sssd-proxy-1.16.1-4.3.2

147705 - SuSE Linux 15.0 openSUSE-SU-2019:0307-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6109, CVE-2019-6111

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0307-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00033.html

SuSE Linux 15.0
x86_64
openssh-debuginfo-7.6p1-lp150.8.15.2
openssh-cavs-7.6p1-lp150.8.15.2
openssh-helpers-7.6p1-lp150.8.15.2
openssh-cavs-debuginfo-7.6p1-lp150.8.15.2
openssh-7.6p1-lp150.8.15.2
openssh-askpass-gnome-debuginfo-7.6p1-lp150.8.15.1
openssh-helpers-debuginfo-7.6p1-lp150.8.15.2
openssh-fips-7.6p1-lp150.8.15.2
openssh-askpass-gnome-7.6p1-lp150.8.15.1
openssh-debugsource-7.6p1-lp150.8.15.2

i586
openssh-debuginfo-7.6p1-lp150.8.15.2
openssh-cavs-7.6p1-lp150.8.15.2
openssh-helpers-7.6p1-lp150.8.15.2
openssh-cavs-debuginfo-7.6p1-lp150.8.15.2
openssh-7.6p1-lp150.8.15.2
openssh-helpers-debuginfo-7.6p1-lp150.8.15.2
openssh-fips-7.6p1-lp150.8.15.2
openssh-debugsource-7.6p1-lp150.8.15.2

147709 - SuSE Linux 42.3 openSUSE-SU-2019:0306-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14662, CVE-2018-16846, CVE-2018-16889

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0306-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-03/msg00039.html

SuSE Linux 42.3
x86_64
python-rbd-12.2.10+git.1549630712.bb089269ea-21.1
ceph-test-debugsource-12.2.10+git.1549630712.bb089269ea-21.1
python-cephfs-12.2.10+git.1549630712.bb089269ea-21.1
ceph-base-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
librados-devel-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-fuse-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
librgw2-12.2.10+git.1549630712.bb089269ea-21.1

python-rados-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
libradosstriper-devel-12.2.10+git.1549630712.bb089269ea-21.1
libcephfs2-12.2.10+git.1549630712.bb089269ea-21.1
ceph-mon-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-mgr-12.2.10+git.1549630712.bb089269ea-21.1
ceph-mds-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-debugsource-12.2.10+git.1549630712.bb089269ea-21.1
rbd-nbd-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
rbd-fuse-12.2.10+git.1549630712.bb089269ea-21.1
python3-ceph-argparse-12.2.10+git.1549630712.bb089269ea-21.1
librbd1-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
librbd1-12.2.10+git.1549630712.bb089269ea-21.1
ceph-resource-agents-12.2.10+git.1549630712.bb089269ea-21.1
python-rados-12.2.10+git.1549630712.bb089269ea-21.1
librgw2-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-osd-12.2.10+git.1549630712.bb089269ea-21.1
librados2-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-mds-12.2.10+git.1549630712.bb089269ea-21.1
python-rgw-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-test-12.2.10+git.1549630712.bb089269ea-21.1
ceph-12.2.10+git.1549630712.bb089269ea-21.1
libcephfs-devel-12.2.10+git.1549630712.bb089269ea-21.1
ceph-radosgw-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
python3-rbd-12.2.10+git.1549630712.bb089269ea-21.1
python3-rados-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-common-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
python3-cephfs-12.2.10+git.1549630712.bb089269ea-21.1
ceph-fuse-12.2.10+git.1549630712.bb089269ea-21.1
ceph-mon-12.2.10+git.1549630712.bb089269ea-21.1
rbd-mirror-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
python-ceph-compat-12.2.10+git.1549630712.bb089269ea-21.1
python-cephfs-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
libcephfs2-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
rbd-nbd-12.2.10+git.1549630712.bb089269ea-21.1
python3-rgw-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
python3-cephfs-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
rbd-fuse-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
rbd-mirror-12.2.10+git.1549630712.bb089269ea-21.1
librbd-devel-12.2.10+git.1549630712.bb089269ea-21.1
python-rgw-12.2.10+git.1549630712.bb089269ea-21.1
libradosstriper1-12.2.10+git.1549630712.bb089269ea-21.1
ceph-base-12.2.10+git.1549630712.bb089269ea-21.1
ceph-radosgw-12.2.10+git.1549630712.bb089269ea-21.1
python3-rbd-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
python3-rgw-12.2.10+git.1549630712.bb089269ea-21.1
librgw-devel-12.2.10+git.1549630712.bb089269ea-21.1
ceph-test-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
python-rbd-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
ceph-mgr-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
librados-devel-12.2.10+git.1549630712.bb089269ea-21.1
ceph-osd-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
libradosstriper1-debuginfo-12.2.10+git.1549630712.bb089269ea-21.1
rados-objclass-devel-12.2.10+git.1549630712.bb089269ea-21.1
librados2-12.2.10+git.1549630712.bb089269ea-21.1
ceph-common-12.2.10+git.1549630712.bb089269ea-21.1
python3-rados-12.2.10+git.1549630712.bb089269ea-21.1

163821 - Oracle Enterprise Linux ELSA-2019-0482 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3804

Description

The scan detected that the host is missing the following update:
ELSA-2019-0482

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008526.html

OEL7
x86_64
cockpit-bridge-173.2-1.0.1.el7
cockpit-machines-ovirt-173.2-1.0.1.el7
cockpit-173.2-1.0.1.el7
cockpit-doc-173.2-1.0.1.el7
cockpit-system-173.2-1.0.1.el7
cockpit-ws-173.2-1.0.1.el7

171073 - Amazon Linux AMI ALAS-2019-1166 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1166.html

Amazon Linux AMI
i686
mod24_md-2.4.38-1.86.amzn1
httpd24-debuginfo-2.4.38-1.86.amzn1
httpd24-devel-2.4.38-1.86.amzn1
mod24_session-2.4.38-1.86.amzn1
httpd24-2.4.38-1.86.amzn1
mod24_ssl-2.4.38-1.86.amzn1
mod24_proxy_html-2.4.38-1.86.amzn1
mod24_ldap-2.4.38-1.86.amzn1
httpd24-tools-2.4.38-1.86.amzn1

noarch
httpd24-manual-2.4.38-1.86.amzn1

x86_64
mod24_md-2.4.38-1.86.amzn1
httpd24-debuginfo-2.4.38-1.86.amzn1
httpd24-devel-2.4.38-1.86.amzn1

mod24_session-2.4.38-1.86.amzn1
httpd24-2.4.38-1.86.amzn1
mod24_ssl-2.4.38-1.86.amzn1
mod24_ldap-2.4.38-1.86.amzn1
mod24_proxy_html-2.4.38-1.86.amzn1
httpd24-tools-2.4.38-1.86.amzn1

178698 - Gentoo Linux GLSA-201903-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-02

Observation

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

https://security.gentoo.org/glsa/201903-02

Affected packages:
app-shells/zsh < 5.6

178699 - Gentoo Linux GLSA-201903-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-08

Observation

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

https://security.gentoo.org/glsa/201903-08

Affected packages:
net-misc/wget < 1.20.1

178700 - Gentoo Linux GLSA-201903-05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-05

Observation

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

https://security.gentoo.org/glsa/201903-05

Affected packages:
app-arch/tar < 1.30-r1

178701 - Gentoo Linux GLSA-201903-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-04

Observation

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

https://security.gentoo.org/glsa/201903-04

Affected packages:
www-client/firefox < 60.5.1
www-client/firefox-bin < 60.5.1

178702 - Gentoo Linux GLSA-201903-06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-06

Observation

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

https://security.gentoo.org/glsa/201903-06

Affected packages:
net-misc/rdesktop < 1.8.4

178703 - Gentoo Linux GLSA-201903-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-03

Observation

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

https://security.gentoo.org/glsa/201903-03

Affected packages:
net-misc/curl < 7.64.0

178704 - Gentoo Linux GLSA-201903-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-07

Observation

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

https://security.gentoo.org/glsa/201903-07

Affected packages:
sys-apps/systemd < 239-r4

178705 - Gentoo Linux GLSA-201903-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-01

Observation

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

https://security.gentoo.org/glsa/201903-01

Affected packages:
sys-cluster/keepalived < 2.0.10

182927 - FreeBSD OpenSSL ChaCha20-Poly1305 Nonce Vulnerability (e56f2f7c-410e-11e9-b95c-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2019-1543

Description

The scan detected that the host is missing the following update:
OpenSSL -- ChaCha20-Poly1305 nonce vulnerability (e56f2f7c-410e-11e9-b95c-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/e56f2f7c-410e-11e9-b95c-b499baebfeaf.html

Affected packages:
openssl111 < 1.1.1b_1

194857 - Fedora Linux 29 FEDORA-2019-c692dd910d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1340

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c692dd910d

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/2019/3/?count=200&page=1

Fedora Core 29

guacamole-server-1.0.0-1.fc29

194864 - Fedora Linux 29 FEDORA-2019-0c1d62bf5b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2922

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0c1d62bf5b

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

Fedora Core 29

drupal7-7.64-1.fc29

194865 - Fedora Linux 28 FEDORA-2019-6c52489ec5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1340

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6c52489ec5

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/2019/3/?count=200&page=1

Fedora Core 28

guacamole-server-1.0.0-1.fc28

24792 - IBM WebSphere Application Server Weaker Than Expected Security Vulnerability (ibm10793421)

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

Risk Level: Medium

CVE: CVE-2018-1996

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw is due to improper TLS configuration. Successful exploitation could allow a remote attacker to disclose sensitive information on the target system.

147697 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0582-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13672, CVE-2017-13673, CVE-2018-16872, CVE-2018-18954, CVE-2018-19364, CVE-2018-19489, CVE-2018-7858, CVE-2019-6778

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0582-1

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-March/005184.html

SuSE SLED 12 SP3
x86_64
qemu-x86-2.9.1-6.28.1
qemu-block-curl-debuginfo-2.9.1-6.28.1
qemu-debugsource-2.9.1-6.28.1
qemu-block-curl-2.9.1-6.28.1
qemu-tools-debuginfo-2.9.1-6.28.1
qemu-kvm-2.9.1-6.28.1
qemu-tools-2.9.1-6.28.1
qemu-2.9.1-6.28.1

noarch
qemu-ipxe-1.0.0+-6.28.1
qemu-sgabios-8-6.28.1
qemu-seabios-1.10.2-6.28.1
qemu-vgabios-1.10.2-6.28.1

SuSE SLES 12 SP3
noarch
qemu-ipxe-1.0.0+-6.28.1
qemu-sgabios-8-6.28.1
qemu-seabios-1.10.2-6.28.1
qemu-vgabios-1.10.2-6.28.1

x86_64
qemu-x86-2.9.1-6.28.1
qemu-guest-agent-2.9.1-6.28.1
qemu-block-ssh-debuginfo-2.9.1-6.28.1
qemu-block-iscsi-debuginfo-2.9.1-6.28.1
qemu-tools-debuginfo-2.9.1-6.28.1
qemu-block-ssh-2.9.1-6.28.1
qemu-block-rbd-debuginfo-2.9.1-6.28.1
qemu-block-iscsi-2.9.1-6.28.1
qemu-block-curl-2.9.1-6.28.1
qemu-kvm-2.9.1-6.28.1
qemu-2.9.1-6.28.1
qemu-x86-debuginfo-2.9.1-6.28.1
qemu-debugsource-2.9.1-6.28.1
qemu-block-curl-debuginfo-2.9.1-6.28.1
qemu-block-rbd-2.9.1-6.28.1
qemu-lang-2.9.1-6.28.1
qemu-tools-2.9.1-6.28.1
qemu-guest-agent-debuginfo-2.9.1-6.28.1

147703 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0572-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1559

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0572-1

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-March/005177.html

SuSE SLED 12 SP4
x86_64
libopenssl1_0_0-32bit-1.0.2p-3.6.1
openssl-1_0_0-debuginfo-1.0.2p-3.6.1
openssl-1_0_0-debugsource-1.0.2p-3.6.1
libopenssl-1_0_0-devel-1.0.2p-3.6.1
libopenssl1_0_0-debuginfo-1.0.2p-3.6.1
libopenssl1_0_0-1.0.2p-3.6.1
openssl-1_0_0-1.0.2p-3.6.1
libopenssl1_0_0-debuginfo-32bit-1.0.2p-3.6.1

SuSE SLES 12 SP4
noarch
openssl-1_0_0-doc-1.0.2p-3.6.1

x86_64
libopenssl1_0_0-hmac-1.0.2p-3.6.1
libopenssl1_0_0-32bit-1.0.2p-3.6.1
libopenssl1_0_0-hmac-32bit-1.0.2p-3.6.1
openssl-1_0_0-debuginfo-1.0.2p-3.6.1
openssl-1_0_0-debugsource-1.0.2p-3.6.1
libopenssl-1_0_0-devel-1.0.2p-3.6.1
libopenssl1_0_0-debuginfo-1.0.2p-3.6.1
libopenssl1_0_0-1.0.2p-3.6.1
openssl-1_0_0-1.0.2p-3.6.1
libopenssl1_0_0-debuginfo-32bit-1.0.2p-3.6.1

160528 - CentOS 7 CESA-2019-0230 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
CESA-2019-0230

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-March/023215.html

CentOS 7
i686
polkit-devel-0.112-18.el7_6.1
polkit-0.112-18.el7_6.1

noarch
polkit-docs-0.112-18.el7_6.1

x86_64
polkit-devel-0.112-18.el7_6.1
polkit-0.112-18.el7_6.1

160529 - CentOS 6 CESA-2019-0462 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
CESA-2019-0462

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-March/023216.html

CentOS 6
i686
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10

noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el6_10

x86_64
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10

182928 - FreeBSD rt XSS Via JQuery (416ca0f4-3fe0-11e9-bbdd-6805ca0b3d42)

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

Risk Level: Medium

CVE: CVE-2015-9251

Description

The scan detected that the host is missing the following update:
rt -- XSS via jQuery (416ca0f4-3fe0-11e9-bbdd-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/416ca0f4-3fe0-11e9-bbdd-6805ca0b3d42.html

Affected packages:
4.2.0 <= rt42 < 4.2.16
4.4.0 <= rt44 < 4.4.4

186603 - Ubuntu Linux 14.04 USN-3908-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3908-1

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-March/004799.html

Ubuntu 14.04

linux-image-powerpc64-smp_3.13.0.166.177
linux-image-generic-lpae_3.13.0.166.177
linux-image-3.13.0-166-powerpc-e500_3.13.0-166.216
linux-image-powerpc-e500_3.13.0.166.177
linux-image-lowlatency_3.13.0.166.177
linux-image-3.13.0-166-lowlatency_3.13.0-166.216
linux-image-3.13.0-166-powerpc-smp_3.13.0-166.216
linux-image-3.13.0-166-powerpc64-emb_3.13.0-166.216
linux-image-generic_3.13.0.166.177
linux-image-3.13.0-166-generic_3.13.0-166.216
linux-image-powerpc-e500mc_3.13.0.166.177
linux-image-3.13.0-166-powerpc64-smp_3.13.0-166.216
linux-image-powerpc-smp_3.13.0.166.177
linux-image-3.13.0-166-powerpc-e500mc_3.13.0-166.216
linux-image-3.13.0-166-generic-lpae_3.13.0-166.216
linux-image-powerpc64-emb_3.13.0.166.177
linux-image-virtual_3.13.0.166.177

194854 - Fedora Linux 28 FEDORA-2019-fc866e9156 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15587

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fc866e9156

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/2019/3/?count=200&page=2

Fedora Core 28

evolution-3.28.5-3.fc28

194855 - Fedora Linux 29 FEDORA-2019-ae7f274d24 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17960, CVE-2018-9861

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ae7f274d24

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

Fedora Core 29

ckeditor-4.11.2-1.fc29

194860 - Fedora Linux 28 FEDORA-2019-009fdcfb60 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000162

Description

The scan detected that the host is missing the following update:
FEDORA-2019-009fdcfb60

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/2019/3/?count=200&page=2

Fedora Core 28

php-erusev-parsedown-1.7.1-1.fc28

194861 - Fedora Linux 29 FEDORA-2019-b02e9bf467 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000162

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b02e9bf467

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

Fedora Core 29

php-erusev-parsedown-1.7.1-1.fc29

194875 - Fedora Linux 28 FEDORA-2019-31ad8a36d8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17960, CVE-2018-9861

Description

The scan detected that the host is missing the following update:
FEDORA-2019-31ad8a36d8

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/2019/3/?count=200&page=2

Fedora Core 28

ckeditor-4.11.2-1.fc28

24824 - (MSPT-Mar2019) Microsoft Team Foundation Server Cross-site Scripting Vulnerability (CVE-2019-0777)

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

Risk Level: Low

CVE: CVE-2019-0777

Description

A vulnerability in some versions of Microsoft 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 input. 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.

89009 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-067-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
SSA:2019-067-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.435412

Slackware 14.0
x86_64
ntp-4.2.8p13-x86_64-1

Slackware 14.2
x86_64
ntp-4.2.8p13-x86_64-1

i586
ntp-4.2.8p13-i586-1

Slackware 14.1
x86_64
ntp-4.2.8p13-x86_64-1

131310 - Debian Linux 9.0 DSA-4407-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9628

Description

The scan detected that the host is missing the following update:
DSA-4407-1

Observation

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

http://www.debian.org/security/2019/dsa-4407

Debian 9.0
all
libxmltooling7_1.6.0-4+deb9u2
xmltooling-schemas_1.6.0-4+deb9u2
libxmltooling-doc_1.6.0-4+deb9u2
libxmltooling-dev_1.6.0-4+deb9u2

131311 - Debian Linux 9.0 DSA-4406-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0804

Description

The scan detected that the host is missing the following update:
DSA-4406-1

Observation

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

http://www.debian.org/security/2019/dsa-4406

Debian 9.0

all
waagent_2.2.18-3~deb9u2

182929 - FreeBSD ntp Crafted Null Dereference Attack From A Trusted Source With An Authenticated Mode 6 Packet (c2576e14-36e2-11e9-9eda-2

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

Risk Level: Low

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
ntp -- Crafted null dereference attack from a trusted source with an authenticated mode 6 packet (c2576e14-36e2-11e9-9eda-206a8a720317)

Observation

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

http://www.vuxml.org/freebsd/c2576e14-36e2-11e9-9eda-206a8a720317.html

Affected packages:
ntp < 4.2.8p13
12.0 <= FreeBSD < 12.0_2
11.2 <= FreeBSD < 11.2_8

186599 - Ubuntu Linux 18.04, 18.10 USN-3904-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3904-1

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-March/004794.html

Ubuntu 18.10

xserver-xorg-video-nvidia-390_390.116-0ubuntu0.18.10.1

Ubuntu 18.04

xserver-xorg-video-nvidia-390_390.116-0ubuntu0.18.04.1

186601 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3907-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0804

Description

The scan detected that the host is missing the following update:
USN-3907-1

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-March/004797.html

Ubuntu 16.04

walinuxagent_2.2.32-0ubuntu1~16.04.2

Ubuntu 18.10

walinuxagent_2.2.32-0ubuntu1~18.10.2

Ubuntu 14.04

walinuxagent_2.2.32-0ubuntu1~14.04.2

Ubuntu 18.04

walinuxagent_2.2.32-0ubuntu1~18.04.2

194851 - Fedora Linux 28 FEDORA-2019-541e91b477 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-2019-541e91b477

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/2019/3/?count=200&page=2

Fedora Core 28

ignition-0.31.0-1.gitf59a653.fc28

194863 - Fedora Linux 29 FEDORA-2019-55788aeb71 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-2019-55788aeb71

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

Fedora Core 29

drupal7-link-1.6-1.fc29

194866 - Fedora Linux 28 FEDORA-2019-f142d69d4b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1002161

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f142d69d4b

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/2019/3/?count=200&page=2

Fedora Core 28

koji-1.16.2-1.fc28

194867 - Fedora Linux 29 FEDORA-2019-7ad9201e59 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-2019-7ad9201e59

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/2019/3/?count=200&page=2

Fedora Core 29

firefox-65.0.2-1.fc29

194871 - Fedora Linux 28 FEDORA-2019-ff4e1a73a5 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-ff4e1a73a5

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/2019/3/?count=200&page=2

Fedora Core 28

drupal7-link-1.6-1.fc28

194872 - Fedora Linux 29 FEDORA-2019-46107f296c 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-2019-46107f296c

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/2019/3/?count=200&page=2

Fedora Core 29

drupal8-8.6.10-1.fc29
php-typo3-phar-stream-wrapper2-2.0.1-1.fc29

194874 - Fedora Linux 29 FEDORA-2019-4debb6711a 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-2019-4debb6711a

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

Fedora Core 29

ignition-0.31.0-1.gitf59a653.fc29

194876 - Fedora Linux 29 FEDORA-2019-9a6906a128 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-17937

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9a6906a128

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

Fedora Core 29

gpsd-3.17-6.fc29

194880 - Fedora Linux 28 FEDORA-2019-3ee66c2020 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-17937

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3ee66c2020

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/2019/3/?count=200&page=2

Fedora Core 28

gpsd-3.17-6.fc28

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.

182918 - FreeBSD OpenSSL Undisclosed Vulnerability (7700061f-34f7-11e9-b95c-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2019-1559

Update Details

FASLScript is updated

194841 - Fedora Linux 28 FEDORA-2019-f0add5eed0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5704

Update Details

CVE is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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