2020-MAY-19
FSL version 7.6.160

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

26543 - (APSB20-24) Vulnerability In Adobe Acrobat and Reader

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

Risk Level: High

CVE: CVE-2020-9592, CVE-2020-9593, CVE-2020-9594, CVE-2020-9595, CVE-2020-9596, CVE-2020-9597, CVE-2020-9598, CVE-2020-9599, CVE-2020-9600, CVE-2020-9601, CVE-2020-9602, CVE-2020-9603, CVE-2020-9604, CVE-2020-9605, CVE-2020-9606, CVE-2020-9607, CVE-2020-9608, CVE-2020-9609, CVE-2020-9610, CVE-2020-9611, CVE-2020-9612, CVE-2020-9613, CVE-2020-9614, CVE-2020-9615

Description

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

Observation

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

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat. The flaws lie in multiple components. Successful exploitation could allow an attacker to escalate privileges, obtain sensitive information, execute arbitrary code, or cause a denial of service condition.

164208 - Oracle Enterprise Linux ELSA-2020-2050 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
ELSA-2020-2050

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009909.html

OEL7
x86_64
thunderbird-68.8.0-1.0.1.el7_8

164211 - Oracle Enterprise Linux ELSA-2020-2046 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
ELSA-2020-2046

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009912.html

OEL8
x86_64
thunderbird-68.8.0-1.0.1.el8_2

164219 - Oracle Enterprise Linux ELSA-2020-2037 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
ELSA-2020-2037

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009891.html

OEL7
x86_64
firefox-68.8.0-1.0.1.el7_8

196723 - Red Hat Enterprise Linux RHSA-2020-2050 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
RHSA-2020-2050

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00020.html

RHEL7D

x86_64
thunderbird-debuginfo-68.8.0-1.el7_8
thunderbird-68.8.0-1.el7_8

RHEL7S
x86_64
thunderbird-debuginfo-68.8.0-1.el7_8
thunderbird-68.8.0-1.el7_8

RHEL7WS
x86_64
thunderbird-debuginfo-68.8.0-1.el7_8
thunderbird-68.8.0-1.el7_8

196728 - Red Hat Enterprise Linux RHSA-2020-2037 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
RHSA-2020-2037

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00010.html

RHEL7D
x86_64
firefox-debuginfo-68.8.0-1.el7_8
firefox-68.8.0-1.el7_8

RHEL7S
x86_64
firefox-debuginfo-68.8.0-1.el7_8
firefox-68.8.0-1.el7_8

RHEL7WS
x86_64
firefox-debuginfo-68.8.0-1.el7_8
firefox-68.8.0-1.el7_8

196730 - Red Hat Enterprise Linux RHSA-2020-2036 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
RHSA-2020-2036

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00011.html

RHEL6D
x86_64
firefox-68.8.0-1.el6_10
firefox-debuginfo-68.8.0-1.el6_10

i386
firefox-68.8.0-1.el6_10
firefox-debuginfo-68.8.0-1.el6_10

RHEL6S
i386
firefox-68.8.0-1.el6_10
firefox-debuginfo-68.8.0-1.el6_10

x86_64
firefox-68.8.0-1.el6_10
firefox-debuginfo-68.8.0-1.el6_10

RHEL6WS
x86_64
firefox-68.8.0-1.el6_10
firefox-debuginfo-68.8.0-1.el6_10

i386
firefox-68.8.0-1.el6_10
firefox-debuginfo-68.8.0-1.el6_10

196732 - Red Hat Enterprise Linux RHSA-2020-2049 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
RHSA-2020-2049

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00019.html

RHEL6S
i386
thunderbird-68.8.0-1.el6_10
thunderbird-debuginfo-68.8.0-1.el6_10

x86_64
thunderbird-68.8.0-1.el6_10
thunderbird-debuginfo-68.8.0-1.el6_10

RHEL6D

x86_64
thunderbird-68.8.0-1.el6_10
thunderbird-debuginfo-68.8.0-1.el6_10

i386
thunderbird-68.8.0-1.el6_10
thunderbird-debuginfo-68.8.0-1.el6_10

RHEL6WS
x86_64
thunderbird-68.8.0-1.el6_10
thunderbird-debuginfo-68.8.0-1.el6_10

i386
thunderbird-68.8.0-1.el6_10
thunderbird-debuginfo-68.8.0-1.el6_10

26511 - (MSPT-May2020) Microsoft SharePoint Remote Code Execution (CVE-2020-1023)

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

Risk Level: High

CVE: CVE-2020-1023

Description

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

Observation

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

The flaw lies in fails to check the source markup. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

26512 - (MSPT-May2020) Microsoft SharePoint Remote Code Execution (CVE-2020-1024)

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

Risk Level: High

CVE: CVE-2020-1024

Description

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

Observation

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

The flaw lies in fails to check the source markup. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

26515 - (MSPT-May2020) Microsoft SharePoint Cross Site Scripting (CVE-2020-1100)

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

Risk Level: High

CVE: CVE-2020-1100

Description

A vulnerability in some versions of Microsoft SharePoint could lead to Cross Site Scripting.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to Cross Site Scripting.

The flaw lies in improperly sanitize crafted web request. Successful exploitation by a remote attacker could result in Cross Site Scripting Attack.

26520 - (MSPT-May2020) Microsoft Windows SharePoint Spoofing (CVE-2020-1105)

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

Risk Level: High

CVE: CVE-2020-1105

Description

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

Observation

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

The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in spoofing

26423 - (MSPT-May2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1114)

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

Risk Level: High

CVE: CVE-2020-1114

Description

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

Observation

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

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

26426 - (MSPT-May2020) Microsoft Windows GDI Privilege Escalation (CVE-2020-1142)

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

Risk Level: High

CVE: CVE-2020-1142

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 GDI 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.

26429 - (MSPT-May2020) Microsoft Windows Graphics Component Privilege Escalation (CVE-2020-1135)

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

Risk Level: High

CVE: CVE-2020-1135

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 Graphics 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.

26431 - (MSPT-May2020) Microsoft WER Improperly Handles and Executes Files Privilege Escalation (CVE-2020-1088)

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

Risk Level: High

CVE: CVE-2020-1088

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 windows error reporting component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26433 - (MSPT-May2020) Microsoft Windows WER Privilege Escalation (CVE-2020-1021)

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

Risk Level: High

CVE: CVE-2020-1021

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 WER 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.

26455 - (MSPT-May2020) Microsoft ICM32.dll Improperly Handles Objects In Memory Remote Code Execution (CVE-2020-1117)

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

Risk Level: High

CVE: CVE-2020-1117

Description

A vulnerability in some versions of Microsoft ICM32.dll could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft ICM32.dll could lead to remote code execution.

The flaw lies in 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.

26456 - (MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1061)

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

Risk Level: High

CVE: CVE-2020-1061

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 in 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.

26460 - (MSPT-May2020) Microsoft Windows Improperly Handles Objects in Memory Denial of Service (CVE-2020-1076)

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

Risk Level: High

CVE: CVE-2020-1076

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 in 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.

26462 - (MSPT-May2020) Microsoft Windows Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1067)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2020-1067

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 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.

26463 - (MSPT-May2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1174)

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

Risk Level: High

CVE: CVE-2020-1174

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.

26464 - (MSPT-May2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1175)

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

Risk Level: High

CVE: CVE-2020-1175

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.

26465 - (MSPT-May2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1176)

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

Risk Level: High

CVE: CVE-2020-1176

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.

26466 - (MSPT-May2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1051)

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

Risk Level: High

CVE: CVE-2020-1051

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.

26467 - (MSPT-May2020) Microsoft Hyper-V Properly Validate Specific Malicious Data Denial of Service (CVE-2020-0909)

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

Risk Level: High

CVE: CVE-2020-0909

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 properly validate specific malicious data. 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.

26468 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1157)

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

Risk Level: High

CVE: CVE-2020-1157

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 Runtime 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.

26469 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1158)

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

Risk Level: High

CVE: CVE-2020-1158

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 Runtime 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.

26474 - (MSPT-May2020) Microsoft MSHTML Improperly Validates Input Remote Code Execution (CVE-2020-1064)

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

Risk Level: High

CVE: CVE-2020-1064

Description

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

Observation

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

The flaw lies in improperly validates 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.

26475 - (MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1035)

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

Risk Level: High

CVE: CVE-2020-1035

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 in 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.

26477 - (MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1058)

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

Risk Level: High

CVE: CVE-2020-1058

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 in 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.

26488 - (MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1060)

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

Risk Level: High

CVE: CVE-2020-1060

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 in 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.

26489 - (MSPT-May2020) Microsoft Internet Explorer Improperly Access Objects in Memory Remote Code Execution (CVE-2020-1062)

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

Risk Level: High

CVE: CVE-2020-1062

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 improperly access 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.

26491 - (MSPT-May2020) Microsoft Internet Explorer Improperly Accesses Objects in Memory Remote Code Execution (CVE-2020-1092)

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

Risk Level: High

CVE: CVE-2020-1092

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

26492 - (MSPT-May2020) Microsoft Internet Explorer Improperly Accesses Objects in Memory Remote Code Execution (CVE-2020-1093)

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

Risk Level: High

CVE: CVE-2020-1093

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

26508 - (MSPT-May2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1087)

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

Risk Level: High

CVE: CVE-2020-1087

Description

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

Observation

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

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

26510 - (MSPT-May2020) Microsoft Excel Remote Code Execution (CVE-2020-0901)

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

Risk Level: High

CVE: CVE-2020-0901

Description

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

Observation

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

The flaw lies in improperly handle 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.

26513 - (MSPT-May2020) Microsoft SharePoint Server Remote Code Execution (CVE-2020-1069)

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

Risk Level: High

CVE: CVE-2020-1069

Description

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

Observation

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

The flaw lies in the ASP.Net component. Successful exploitation by an attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

26517 - (MSPT-May2020) Microsoft Windows SharePoint Remote Code Execution (CVE-2020-1102)

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

Risk Level: High

CVE: CVE-2020-1102

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 SharePoint component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

26527 - (MSPT-May2020) Microsoft Windows Graphics Components Remote Code Execution (CVE-2020-1153)

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

Risk Level: High

CVE: CVE-2020-1153

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 Graphics Components 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.

148950 - SuSE Linux 15.1 openSUSE-SU-2020:0620-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-6464, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0620-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00081.html

SuSE Linux 15.1
x86_64
chromium-debugsource-81.0.4044.138-lp151.2.88.1
chromedriver-debuginfo-81.0.4044.138-lp151.2.88.1
chromium-debuginfo-81.0.4044.138-lp151.2.88.1
chromedriver-81.0.4044.138-lp151.2.88.1
chromium-81.0.4044.138-lp151.2.88.1

148951 - SuSE SLES 12 SP4, 12 SP5 SUSE-SU-2020:1212-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12268

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1212-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006798.html

SuSE SLES 12 SP4
x86_64
ghostscript-x11-debuginfo-9.52-23.34.1
libspectre-debugsource-0.2.7-12.10.1
ghostscript-9.52-23.34.1
libspectre1-0.2.7-12.10.1
ghostscript-debuginfo-9.52-23.34.1
ghostscript-x11-9.52-23.34.1
ghostscript-debugsource-9.52-23.34.1
libspectre1-debuginfo-0.2.7-12.10.1

SuSE SLES 12 SP5
x86_64
ghostscript-x11-debuginfo-9.52-23.34.1
libspectre-debugsource-0.2.7-12.10.1
ghostscript-9.52-23.34.1
libspectre1-0.2.7-12.10.1
ghostscript-debuginfo-9.52-23.34.1
ghostscript-x11-9.52-23.34.1
ghostscript-debugsource-9.52-23.34.1
libspectre1-debuginfo-0.2.7-12.10.1

148952 - SuSE Linux 15.1 openSUSE-SU-2020:0654-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-7106

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0654-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00088.html
https://lists.opensuse.org/opensuse-updates/2020-05/msg00086.html

SuSE Linux 15.1
x86_64
cacti-1.2.12-bp151.4.9.1
cacti-spine-debugsource-1.2.12-lp151.3.9.1
cacti-spine-debuginfo-1.2.12-lp151.3.9.1
cacti-spine-1.2.12-lp151.3.9.1

noarch
cacti-spine-1.2.12-bp151.4.9.1
cacti-1.2.12-lp151.3.9.1

148953 - SuSE Linux 15.1 openSUSE-SU-2020:0623-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-12519, CVE-2019-12521, CVE-2019-12528, CVE-2019-18860, CVE-2020-11945, CVE-2020-8517

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0623-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00060.html

SuSE Linux 15.1

x86_64
squid-4.11-lp151.2.15.2
squid-debuginfo-4.11-lp151.2.15.2
squid-debugsource-4.11-lp151.2.15.2

148954 - SuSE Linux 15.1 openSUSE-SU-2020:0622-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-14559

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0622-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00063.html

SuSE Linux 15.1
i586
ovmf-2017+git1510945757.b2662641d5-lp151.11.6.1
ovmf-tools-2017+git1510945757.b2662641d5-lp151.11.6.1

noarch
qemu-ovmf-ia32-2017+git1510945757.b2662641d5-lp151.11.6.1
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-lp151.11.6.1

x86_64
qemu-ovmf-x86_64-debug-2017+git1510945757.b2662641d5-lp151.11.6.1
ovmf-2017+git1510945757.b2662641d5-lp151.11.6.1
ovmf-tools-2017+git1510945757.b2662641d5-lp151.11.6.1

148955 - SuSE SLES 12 SP5 SUSE-SU-2020:1277-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10703, CVE-2020-12430

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1277-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006819.html

SuSE SLES 12 SP5
x86_64
libvirt-lock-sanlock-5.1.0-13.6.2
libvirt-daemon-driver-storage-mpath-5.1.0-13.6.2
libvirt-daemon-driver-libxl-debuginfo-5.1.0-13.6.2

libvirt-daemon-lxc-5.1.0-13.6.2
libvirt-daemon-driver-nwfilter-5.1.0-13.6.2
libvirt-libs-5.1.0-13.6.2
libvirt-daemon-driver-storage-disk-5.1.0-13.6.2
libvirt-admin-5.1.0-13.6.2
libvirt-daemon-driver-storage-scsi-5.1.0-13.6.2
libvirt-daemon-driver-storage-rbd-debuginfo-5.1.0-13.6.2
libvirt-daemon-xen-5.1.0-13.6.2
libvirt-daemon-driver-storage-rbd-5.1.0-13.6.2
libvirt-nss-debuginfo-5.1.0-13.6.2
libvirt-client-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-nodedev-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-nwfilter-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-nodedev-5.1.0-13.6.2
libvirt-daemon-driver-lxc-debuginfo-5.1.0-13.6.2
libvirt-daemon-qemu-5.1.0-13.6.2
libvirt-5.1.0-13.6.2
libvirt-daemon-driver-storage-disk-debuginfo-5.1.0-13.6.2
libvirt-client-5.1.0-13.6.2
libvirt-libs-debuginfo-5.1.0-13.6.2
libvirt-admin-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-lxc-5.1.0-13.6.2
libvirt-daemon-driver-storage-scsi-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-secret-5.1.0-13.6.2
libvirt-daemon-driver-storage-5.1.0-13.6.2
libvirt-lock-sanlock-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-qemu-5.1.0-13.6.2
libvirt-daemon-driver-interface-debuginfo-5.1.0-13.6.2
libvirt-daemon-config-network-5.1.0-13.6.2
libvirt-daemon-driver-network-5.1.0-13.6.2
libvirt-debugsource-5.1.0-13.6.2
libvirt-doc-5.1.0-13.6.2
libvirt-daemon-driver-libxl-5.1.0-13.6.2
libvirt-daemon-driver-interface-5.1.0-13.6.2
libvirt-daemon-driver-secret-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-storage-iscsi-5.1.0-13.6.2
libvirt-daemon-driver-storage-logical-debuginfo-5.1.0-13.6.2
libvirt-daemon-config-nwfilter-5.1.0-13.6.2
libvirt-daemon-5.1.0-13.6.2
libvirt-daemon-driver-network-debuginfo-5.1.0-13.6.2
libvirt-daemon-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-storage-mpath-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-qemu-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-storage-logical-5.1.0-13.6.2
libvirt-nss-5.1.0-13.6.2
libvirt-daemon-hooks-5.1.0-13.6.2
libvirt-daemon-driver-storage-iscsi-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-storage-core-debuginfo-5.1.0-13.6.2
libvirt-daemon-driver-storage-core-5.1.0-13.6.2

148956 - SuSE Linux 15.1 openSUSE-SU-2020:0651-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-11888

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0651-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00084.html

SuSE Linux 15.1
noarch
python2-markdown2-2.3.7-lp151.2.3.1
python3-markdown2-2.3.7-lp151.2.3.1

148957 - SuSE SLES 12 SP4, 12 SP5, SLED 12 SP4 SUSE-SU-2020:1211-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-3899

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1211-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006800.html

SuSE SLES 12 SP4
noarch
libwebkit2gtk3-lang-2.28.2-2.53.2

x86_64
webkit2gtk-4_0-injected-bundles-2.28.2-2.53.2
libjavascriptcoregtk-4_0-18-debuginfo-2.28.2-2.53.2
typelib-1_0-JavaScriptCore-4_0-2.28.2-2.53.2
typelib-1_0-WebKit2-4_0-2.28.2-2.53.2
webkit2gtk3-debugsource-2.28.2-2.53.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.28.2-2.53.2
libwebkit2gtk-4_0-37-debuginfo-2.28.2-2.53.2
libjavascriptcoregtk-4_0-18-2.28.2-2.53.2
libwebkit2gtk-4_0-37-2.28.2-2.53.2

SuSE SLED 12 SP4
noarch
libwebkit2gtk3-lang-2.28.2-2.53.2

SuSE SLES 12 SP5
noarch
libwebkit2gtk3-lang-2.28.2-2.53.2

x86_64
webkit2gtk-4_0-injected-bundles-2.28.2-2.53.2
libjavascriptcoregtk-4_0-18-debuginfo-2.28.2-2.53.2
webkit2gtk3-debugsource-2.28.2-2.53.2
typelib-1_0-JavaScriptCore-4_0-2.28.2-2.53.2
typelib-1_0-WebKit2-4_0-2.28.2-2.53.2
typelib-1_0-WebKit2WebExtension-4_0-2.28.2-2.53.2

webkit2gtk-4_0-injected-bundles-debuginfo-2.28.2-2.53.2
libwebkit2gtk-4_0-37-debuginfo-2.28.2-2.53.2
libjavascriptcoregtk-4_0-18-2.28.2-2.53.2
libwebkit2gtk-4_0-37-2.28.2-2.53.2

148958 - SuSE Linux 15.1 openSUSE-SU-2020:0653-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12268

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0653-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00089.html

SuSE Linux 15.1
x86_64
ghostscript-mini-9.52-lp151.3.12.1
ghostscript-debuginfo-9.52-lp151.3.12.1
ghostscript-devel-9.52-lp151.3.12.1
libspectre-devel-0.2.8-lp151.3.3.1
libspectre-debugsource-0.2.8-lp151.3.3.1
ghostscript-x11-9.52-lp151.3.12.1
libspectre1-0.2.8-lp151.3.3.1
ghostscript-debugsource-9.52-lp151.3.12.1
ghostscript-mini-devel-9.52-lp151.3.12.1
ghostscript-mini-debuginfo-9.52-lp151.3.12.1
ghostscript-mini-debugsource-9.52-lp151.3.12.1
libspectre1-debuginfo-0.2.8-lp151.3.3.1
ghostscript-x11-debuginfo-9.52-lp151.3.12.1
ghostscript-9.52-lp151.3.12.1

i586
ghostscript-devel-9.52-lp151.3.12.1
ghostscript-x11-9.52-lp151.3.12.1
ghostscript-mini-debuginfo-9.52-lp151.3.12.1
ghostscript-debuginfo-9.52-lp151.3.12.1
ghostscript-mini-devel-9.52-lp151.3.12.1
ghostscript-9.52-lp151.3.12.1
ghostscript-mini-9.52-lp151.3.12.1
ghostscript-mini-debugsource-9.52-lp151.3.12.1
ghostscript-x11-debuginfo-9.52-lp151.3.12.1
ghostscript-debugsource-9.52-lp151.3.12.1

148959 - SuSE Linux 15.1 openSUSE-SU-2020:0628-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12050

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0628-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00077.html

SuSE Linux 15.1
x86_64
sqliteodbc-doc-0.9996-lp151.3.3.1
sqliteodbc-0.9996-lp151.3.3.1
sqliteodbc-debugsource-0.9996-lp151.3.3.1
sqliteodbc-debuginfo-0.9996-lp151.3.3.1

148960 - SuSE SLES 12 SP4 SUSE-SU-2020:1289-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10703

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1289-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006821.html

SuSE SLES 12 SP4
x86_64
libvirt-daemon-driver-storage-logical-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-logical-4.0.0-8.20.2
libvirt-lock-sanlock-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-4.0.0-8.20.2
libvirt-daemon-driver-nwfilter-4.0.0-8.20.2
libvirt-libs-debuginfo-4.0.0-8.20.2
libvirt-daemon-lxc-4.0.0-8.20.2
libvirt-debugsource-4.0.0-8.20.2
libvirt-daemon-xen-4.0.0-8.20.2
libvirt-daemon-hooks-4.0.0-8.20.2
libvirt-daemon-driver-network-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-iscsi-4.0.0-8.20.2
libvirt-daemon-qemu-4.0.0-8.20.2
libvirt-daemon-driver-secret-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-interface-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-libxl-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-nwfilter-debuginfo-4.0.0-8.20.2
libvirt-lock-sanlock-4.0.0-8.20.2
libvirt-client-4.0.0-8.20.2
libvirt-daemon-driver-qemu-4.0.0-8.20.2
libvirt-daemon-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-secret-4.0.0-8.20.2
libvirt-daemon-driver-storage-rbd-debuginfo-4.0.0-8.20.2

libvirt-daemon-driver-libxl-4.0.0-8.20.2
libvirt-daemon-config-nwfilter-4.0.0-8.20.2
libvirt-daemon-driver-lxc-4.0.0-8.20.2
libvirt-daemon-driver-storage-mpath-debuginfo-4.0.0-8.20.2
libvirt-nss-debuginfo-4.0.0-8.20.2
libvirt-doc-4.0.0-8.20.2
libvirt-4.0.0-8.20.2
libvirt-daemon-driver-storage-core-4.0.0-8.20.2
libvirt-daemon-driver-storage-rbd-4.0.0-8.20.2
libvirt-daemon-driver-network-4.0.0-8.20.2
libvirt-daemon-driver-nodedev-4.0.0-8.20.2
libvirt-daemon-driver-storage-mpath-4.0.0-8.20.2
libvirt-daemon-driver-storage-scsi-4.0.0-8.20.2
libvirt-nss-4.0.0-8.20.2
libvirt-daemon-driver-storage-scsi-debuginfo-4.0.0-8.20.2
libvirt-admin-4.0.0-8.20.2
libvirt-client-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-interface-4.0.0-8.20.2
libvirt-daemon-config-network-4.0.0-8.20.2
libvirt-libs-4.0.0-8.20.2
libvirt-daemon-driver-lxc-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-iscsi-debuginfo-4.0.0-8.20.2
libvirt-daemon-4.0.0-8.20.2
libvirt-daemon-driver-qemu-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-disk-4.0.0-8.20.2
libvirt-admin-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-core-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-nodedev-debuginfo-4.0.0-8.20.2
libvirt-daemon-driver-storage-disk-debuginfo-4.0.0-8.20.2

148961 - SuSE Linux 15.1 openSUSE-SU-2020:0631-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0631-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00070.html

SuSE Linux 15.1
i586
rpmlint-mini-debuginfo-1.10-lp151.5.13.1
rpmlint-mini-1.10-lp151.5.13.1
rpmlint-mini-debugsource-1.10-lp151.5.13.1

noarch
rpmlint-1.10-lp151.9.6.1

x86_64
rpmlint-tests-debugsource-84.87+git20181018.60e0249-lp151.9.6.1
rpmlint-mini-debuginfo-1.10-lp151.5.13.1

rpmlint-mini-1.10-lp151.5.13.1
rpmlint-mini-debugsource-1.10-lp151.5.13.1

148962 - SuSE Linux 15.1 openSUSE-SU-2020:0636-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1983

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0636-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00065.html

SuSE Linux 15.1
x86_64
slirp4netns-0.4.5-lp151.2.9.1
slirp4netns-debuginfo-0.4.5-lp151.2.9.1
slirp4netns-debugsource-0.4.5-lp151.2.9.1

148963 - SuSE Linux 15.1 openSUSE-SU-2020:0630-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1747

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0630-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00056.html

SuSE Linux 15.1
x86_64
python3-PyYAML-debuginfo-5.1.2-lp151.2.13.1
python2-PyYAML-5.1.2-lp151.2.13.1
python3-PyYAML-5.1.2-lp151.2.13.1
python-PyYAML-debuginfo-5.1.2-lp151.2.13.1
python2-PyYAML-debuginfo-5.1.2-lp151.2.13.1
python-PyYAML-debugsource-5.1.2-lp151.2.13.1

i586
python3-PyYAML-debuginfo-5.1.2-lp151.2.13.1
python2-PyYAML-5.1.2-lp151.2.13.1
python3-PyYAML-5.1.2-lp151.2.13.1
python-PyYAML-debuginfo-5.1.2-lp151.2.13.1
python2-PyYAML-debuginfo-5.1.2-lp151.2.13.1

python-PyYAML-debugsource-5.1.2-lp151.2.13.1

148964 - SuSE Linux 15.1 openSUSE-SU-2020:0647-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12243

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0647-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00055.html

SuSE Linux 15.1
i586
openldap2-devel-static-2.4.46-lp151.10.9.1
openldap2-contrib-2.4.46-lp151.10.9.1
openldap2-debuginfo-2.4.46-lp151.10.9.1
openldap2-contrib-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-sock-debuginfo-2.4.46-lp151.10.9.1
openldap2-devel-2.4.46-lp151.10.9.1
openldap2-2.4.46-lp151.10.9.1
openldap2-client-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-meta-debuginfo-2.4.46-lp151.10.9.1
openldap2-debugsource-2.4.46-lp151.10.9.1
openldap2-back-perl-2.4.46-lp151.10.9.1
openldap2-client-2.4.46-lp151.10.9.1
openldap2-back-perl-debuginfo-2.4.46-lp151.10.9.1
openldap2-ppolicy-check-password-debuginfo-1.2-lp151.10.9.1
openldap2-back-sql-2.4.46-lp151.10.9.1
openldap2-ppolicy-check-password-1.2-lp151.10.9.1
openldap2-back-meta-2.4.46-lp151.10.9.1
libldap-2_4-2-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-sock-2.4.46-lp151.10.9.1
openldap2-back-sql-debuginfo-2.4.46-lp151.10.9.1
libldap-2_4-2-2.4.46-lp151.10.9.1

noarch
libldap-data-2.4.46-lp151.10.9.1
openldap2-doc-2.4.46-lp151.10.9.1

x86_64
openldap2-devel-static-2.4.46-lp151.10.9.1
openldap2-contrib-2.4.46-lp151.10.9.1
openldap2-debuginfo-2.4.46-lp151.10.9.1
openldap2-contrib-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-sock-debuginfo-2.4.46-lp151.10.9.1
openldap2-devel-2.4.46-lp151.10.9.1
openldap2-2.4.46-lp151.10.9.1
openldap2-client-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-meta-debuginfo-2.4.46-lp151.10.9.1
openldap2-debugsource-2.4.46-lp151.10.9.1
libldap-2_4-2-32bit-2.4.46-lp151.10.9.1

openldap2-back-perl-2.4.46-lp151.10.9.1
openldap2-client-2.4.46-lp151.10.9.1
openldap2-back-perl-debuginfo-2.4.46-lp151.10.9.1
openldap2-ppolicy-check-password-debuginfo-1.2-lp151.10.9.1
libldap-2_4-2-32bit-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-sql-2.4.46-lp151.10.9.1
openldap2-ppolicy-check-password-1.2-lp151.10.9.1
openldap2-back-meta-2.4.46-lp151.10.9.1
libldap-2_4-2-debuginfo-2.4.46-lp151.10.9.1
openldap2-back-sock-2.4.46-lp151.10.9.1
openldap2-back-sql-debuginfo-2.4.46-lp151.10.9.1
openldap2-devel-32bit-2.4.46-lp151.10.9.1
libldap-2_4-2-2.4.46-lp151.10.9.1

148965 - SuSE Linux 15.1 openSUSE-SU-2020:0646-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-3899

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0646-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00054.html

SuSE Linux 15.1
i586
libwebkit2gtk-4_0-37-2.28.2-lp151.2.18.1
webkit-jsc-4-2.28.2-lp151.2.18.1
webkit2gtk3-minibrowser-debuginfo-2.28.2-lp151.2.18.1
webkit2gtk3-devel-2.28.2-lp151.2.18.1
typelib-1_0-JavaScriptCore-4_0-2.28.2-lp151.2.18.1
libjavascriptcoregtk-4_0-18-debuginfo-2.28.2-lp151.2.18.1
libjavascriptcoregtk-4_0-18-2.28.2-lp151.2.18.1
webkit2gtk3-debugsource-2.28.2-lp151.2.18.1
webkit-jsc-4-debuginfo-2.28.2-lp151.2.18.1
libwebkit2gtk-4_0-37-debuginfo-2.28.2-lp151.2.18.1
typelib-1_0-WebKit2WebExtension-4_0-2.28.2-lp151.2.18.1
typelib-1_0-WebKit2-4_0-2.28.2-lp151.2.18.1
webkit2gtk3-minibrowser-2.28.2-lp151.2.18.1
webkit2gtk-4_0-injected-bundles-2.28.2-lp151.2.18.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.28.2-lp151.2.18.1

noarch
libwebkit2gtk3-lang-2.28.2-lp151.2.18.1

x86_64
libwebkit2gtk-4_0-37-32bit-2.28.2-lp151.2.18.1
libwebkit2gtk-4_0-37-2.28.2-lp151.2.18.1
webkit-jsc-4-2.28.2-lp151.2.18.1
webkit2gtk3-minibrowser-debuginfo-2.28.2-lp151.2.18.1
webkit2gtk3-devel-2.28.2-lp151.2.18.1
typelib-1_0-JavaScriptCore-4_0-2.28.2-lp151.2.18.1

libjavascriptcoregtk-4_0-18-debuginfo-2.28.2-lp151.2.18.1
libjavascriptcoregtk-4_0-18-2.28.2-lp151.2.18.1
webkit2gtk3-debugsource-2.28.2-lp151.2.18.1
webkit-jsc-4-debuginfo-2.28.2-lp151.2.18.1
libwebkit2gtk-4_0-37-debuginfo-2.28.2-lp151.2.18.1
typelib-1_0-WebKit2WebExtension-4_0-2.28.2-lp151.2.18.1
typelib-1_0-WebKit2-4_0-2.28.2-lp151.2.18.1
webkit2gtk3-minibrowser-2.28.2-lp151.2.18.1
libjavascriptcoregtk-4_0-18-32bit-2.28.2-lp151.2.18.1
webkit2gtk-4_0-injected-bundles-2.28.2-lp151.2.18.1
libjavascriptcoregtk-4_0-18-32bit-debuginfo-2.28.2-lp151.2.18.1
libwebkit2gtk-4_0-37-32bit-debuginfo-2.28.2-lp151.2.18.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.28.2-lp151.2.18.1

148966 - SuSE SLES 12 SP4 SUSE-SU-2020:1227-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-12519, CVE-2019-12520, CVE-2019-12521, CVE-2019-12524, CVE-2020-11945

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1227-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006808.html

SuSE SLES 12 SP4
x86_64
squid-debuginfo-3.5.21-26.23.1
squid-3.5.21-26.23.1
squid-debugsource-3.5.21-26.23.1

148967 - SuSE Linux 15.1 openSUSE-SU-2020:0643-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12393, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0643-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00074.html

SuSE Linux 15.1
x86_64
MozillaThunderbird-translations-common-68.8.0-lp151.2.38.2
MozillaThunderbird-translations-other-68.8.0-lp151.2.38.2

MozillaThunderbird-debugsource-68.8.0-lp151.2.38.2
MozillaThunderbird-68.8.0-lp151.2.38.2
MozillaThunderbird-debuginfo-68.8.0-lp151.2.38.2

148968 - SuSE Linux 15.1 openSUSE-SU-2020:0661-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12108

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0661-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00096.html

SuSE Linux 15.1
x86_64
mailman-debuginfo-2.1.29-lp151.3.11.1
mailman-debugsource-2.1.29-lp151.3.11.1
mailman-2.1.29-lp151.3.11.1

148969 - SuSE SLES 12 SP4, 12 SP5 SUSE-SU-2020:1285-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1747

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1285-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006820.html

SuSE SLES 12 SP4
x86_64
python3-PyYAML-debuginfo-5.1.2-26.12.1
python3-PyYAML-5.1.2-26.12.1
python-PyYAML-5.1.2-26.12.1
python-PyYAML-debugsource-5.1.2-26.12.1
python-PyYAML-debuginfo-5.1.2-26.12.1

SuSE SLES 12 SP5
x86_64
python3-PyYAML-debuginfo-5.1.2-26.12.1
python3-PyYAML-5.1.2-26.12.1
python-PyYAML-5.1.2-26.12.1
python-PyYAML-debugsource-5.1.2-26.12.1

python-PyYAML-debuginfo-5.1.2-26.12.1

148970 - SuSE Linux 15.1 openSUSE-SU-2020:0642-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-7064, CVE-2020-7066

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0642-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00076.html

SuSE Linux 15.1
i586
php7-sodium-7.2.5-lp151.6.25.1
php7-opcache-debuginfo-7.2.5-lp151.6.25.1
libtidy-devel-5.4.0-lp151.3.3.1
php7-iconv-debuginfo-7.2.5-lp151.6.25.1
php7-tidy-debuginfo-7.2.5-lp151.6.25.1
php7-gettext-debuginfo-7.2.5-lp151.6.25.1
php7-phar-7.2.5-lp151.6.25.1
php7-sqlite-7.2.5-lp151.6.25.1
php7-enchant-debuginfo-7.2.5-lp151.6.25.1
php7-mbstring-7.2.5-lp151.6.25.1
libtidy5-debuginfo-5.4.0-lp151.3.3.1
php7-readline-7.2.5-lp151.6.25.1
php7-shmop-debuginfo-7.2.5-lp151.6.25.1
php7-posix-debuginfo-7.2.5-lp151.6.25.1
php7-embed-7.2.5-lp151.6.25.1
php7-mbstring-debuginfo-7.2.5-lp151.6.25.1
php7-exif-7.2.5-lp151.6.25.1
php7-sysvshm-7.2.5-lp151.6.25.1
php7-mysql-7.2.5-lp151.6.25.1
php7-snmp-7.2.5-lp151.6.25.1
php7-sockets-debuginfo-7.2.5-lp151.6.25.1
php7-gettext-7.2.5-lp151.6.25.1
php7-zlib-debuginfo-7.2.5-lp151.6.25.1
php7-calendar-debuginfo-7.2.5-lp151.6.25.1
php7-test-7.2.5-lp151.6.25.1
php7-soap-debuginfo-7.2.5-lp151.6.25.1
php7-pdo-7.2.5-lp151.6.25.1
php7-xsl-7.2.5-lp151.6.25.1
php7-fileinfo-debuginfo-7.2.5-lp151.6.25.1
php7-pgsql-debuginfo-7.2.5-lp151.6.25.1
php7-pgsql-7.2.5-lp151.6.25.1
php7-ldap-7.2.5-lp151.6.25.1
php7-devel-7.2.5-lp151.6.25.1
php7-exif-debuginfo-7.2.5-lp151.6.25.1
php7-calendar-7.2.5-lp151.6.25.1
php7-zlib-7.2.5-lp151.6.25.1
php7-gd-7.2.5-lp151.6.25.1
tidy-debugsource-5.4.0-lp151.3.3.1

php7-ctype-debuginfo-7.2.5-lp151.6.25.1
php7-pcntl-debuginfo-7.2.5-lp151.6.25.1
php7-sqlite-debuginfo-7.2.5-lp151.6.25.1
php7-gd-debuginfo-7.2.5-lp151.6.25.1
php7-xmlrpc-debuginfo-7.2.5-lp151.6.25.1
php7-firebird-7.2.5-lp151.6.25.1
php7-intl-debuginfo-7.2.5-lp151.6.25.1
php7-intl-7.2.5-lp151.6.25.1
php7-mysql-debuginfo-7.2.5-lp151.6.25.1
php7-dom-debuginfo-7.2.5-lp151.6.25.1
php7-gmp-debuginfo-7.2.5-lp151.6.25.1
php7-shmop-7.2.5-lp151.6.25.1
php7-tidy-7.2.5-lp151.6.25.1
php7-xmlrpc-7.2.5-lp151.6.25.1
php7-bz2-debuginfo-7.2.5-lp151.6.25.1
php7-curl-debuginfo-7.2.5-lp151.6.25.1
php7-fastcgi-7.2.5-lp151.6.25.1
php7-pcntl-7.2.5-lp151.6.25.1
php7-embed-debuginfo-7.2.5-lp151.6.25.1
php7-soap-7.2.5-lp151.6.25.1
php7-sodium-debuginfo-7.2.5-lp151.6.25.1
tidy-5.4.0-lp151.3.3.1
php7-opcache-7.2.5-lp151.6.25.1
php7-dom-7.2.5-lp151.6.25.1
php7-iconv-7.2.5-lp151.6.25.1
php7-sysvshm-debuginfo-7.2.5-lp151.6.25.1
php7-xmlreader-debuginfo-7.2.5-lp151.6.25.1
php7-ctype-7.2.5-lp151.6.25.1
php7-tokenizer-debuginfo-7.2.5-lp151.6.25.1
php7-json-7.2.5-lp151.6.25.1
php7-readline-debuginfo-7.2.5-lp151.6.25.1
php7-xmlreader-7.2.5-lp151.6.25.1
php7-enchant-7.2.5-lp151.6.25.1
php7-odbc-debuginfo-7.2.5-lp151.6.25.1
tidy-debuginfo-5.4.0-lp151.3.3.1
php7-sockets-7.2.5-lp151.6.25.1
php7-phar-debuginfo-7.2.5-lp151.6.25.1
php7-gmp-7.2.5-lp151.6.25.1
php7-dba-7.2.5-lp151.6.25.1
php7-xsl-debuginfo-7.2.5-lp151.6.25.1
apache2-mod_php7-7.2.5-lp151.6.25.1
php7-snmp-debuginfo-7.2.5-lp151.6.25.1
php7-sysvmsg-debuginfo-7.2.5-lp151.6.25.1
php7-bcmath-7.2.5-lp151.6.25.1
php7-fileinfo-7.2.5-lp151.6.25.1
php7-debugsource-7.2.5-lp151.6.25.1
php7-sysvsem-7.2.5-lp151.6.25.1
php7-wddx-7.2.5-lp151.6.25.1
php7-pdo-debuginfo-7.2.5-lp151.6.25.1
libtidy5-5.4.0-lp151.3.3.1
php7-firebird-debuginfo-7.2.5-lp151.6.25.1
php7-tokenizer-7.2.5-lp151.6.25.1
php7-fastcgi-debuginfo-7.2.5-lp151.6.25.1
php7-openssl-7.2.5-lp151.6.25.1
php7-debuginfo-7.2.5-lp151.6.25.1
php7-xmlwriter-7.2.5-lp151.6.25.1
php7-zip-7.2.5-lp151.6.25.1
php7-fpm-debuginfo-7.2.5-lp151.6.25.1
php7-json-debuginfo-7.2.5-lp151.6.25.1
apache2-mod_php7-debuginfo-7.2.5-lp151.6.25.1

php7-odbc-7.2.5-lp151.6.25.1
php7-wddx-debuginfo-7.2.5-lp151.6.25.1
php7-curl-7.2.5-lp151.6.25.1
php7-openssl-debuginfo-7.2.5-lp151.6.25.1
php7-posix-7.2.5-lp151.6.25.1
php7-ftp-debuginfo-7.2.5-lp151.6.25.1
php7-ldap-debuginfo-7.2.5-lp151.6.25.1
php7-bcmath-debuginfo-7.2.5-lp151.6.25.1
php7-bz2-7.2.5-lp151.6.25.1
php7-sysvmsg-7.2.5-lp151.6.25.1
php7-ftp-7.2.5-lp151.6.25.1
php7-zip-debuginfo-7.2.5-lp151.6.25.1
php7-fpm-7.2.5-lp151.6.25.1
php7-dba-debuginfo-7.2.5-lp151.6.25.1
php7-7.2.5-lp151.6.25.1
php7-xmlwriter-debuginfo-7.2.5-lp151.6.25.1
php7-sysvsem-debuginfo-7.2.5-lp151.6.25.1

noarch
tidy-doc-5.4.0-lp151.3.3.1
php7-pear-7.2.5-lp151.6.25.1
php7-pear-Archive_Tar-7.2.5-lp151.6.25.1

x86_64
php7-sodium-7.2.5-lp151.6.25.1
php7-opcache-debuginfo-7.2.5-lp151.6.25.1
libtidy-devel-5.4.0-lp151.3.3.1
php7-iconv-debuginfo-7.2.5-lp151.6.25.1
php7-tidy-debuginfo-7.2.5-lp151.6.25.1
php7-gettext-debuginfo-7.2.5-lp151.6.25.1
php7-phar-7.2.5-lp151.6.25.1
php7-sqlite-7.2.5-lp151.6.25.1
php7-enchant-debuginfo-7.2.5-lp151.6.25.1
php7-mbstring-7.2.5-lp151.6.25.1
libtidy5-debuginfo-5.4.0-lp151.3.3.1
php7-readline-7.2.5-lp151.6.25.1
php7-shmop-debuginfo-7.2.5-lp151.6.25.1
php7-posix-debuginfo-7.2.5-lp151.6.25.1
php7-embed-7.2.5-lp151.6.25.1
php7-mbstring-debuginfo-7.2.5-lp151.6.25.1
php7-exif-7.2.5-lp151.6.25.1
php7-sysvshm-7.2.5-lp151.6.25.1
php7-mysql-7.2.5-lp151.6.25.1
php7-snmp-7.2.5-lp151.6.25.1
php7-sockets-debuginfo-7.2.5-lp151.6.25.1
php7-gettext-7.2.5-lp151.6.25.1
php7-zlib-debuginfo-7.2.5-lp151.6.25.1
php7-calendar-debuginfo-7.2.5-lp151.6.25.1
php7-test-7.2.5-lp151.6.25.1
php7-soap-debuginfo-7.2.5-lp151.6.25.1
php7-pdo-7.2.5-lp151.6.25.1
php7-xsl-7.2.5-lp151.6.25.1
php7-fileinfo-debuginfo-7.2.5-lp151.6.25.1
php7-pgsql-debuginfo-7.2.5-lp151.6.25.1
php7-pgsql-7.2.5-lp151.6.25.1
php7-ldap-7.2.5-lp151.6.25.1
php7-devel-7.2.5-lp151.6.25.1
php7-exif-debuginfo-7.2.5-lp151.6.25.1
php7-calendar-7.2.5-lp151.6.25.1
php7-zlib-7.2.5-lp151.6.25.1

php7-gd-7.2.5-lp151.6.25.1
tidy-debugsource-5.4.0-lp151.3.3.1
php7-ctype-debuginfo-7.2.5-lp151.6.25.1
php7-pcntl-debuginfo-7.2.5-lp151.6.25.1
php7-sqlite-debuginfo-7.2.5-lp151.6.25.1
php7-gd-debuginfo-7.2.5-lp151.6.25.1
php7-xmlrpc-debuginfo-7.2.5-lp151.6.25.1
php7-firebird-7.2.5-lp151.6.25.1
php7-intl-debuginfo-7.2.5-lp151.6.25.1
php7-intl-7.2.5-lp151.6.25.1
php7-mysql-debuginfo-7.2.5-lp151.6.25.1
php7-dom-debuginfo-7.2.5-lp151.6.25.1
php7-gmp-debuginfo-7.2.5-lp151.6.25.1
php7-shmop-7.2.5-lp151.6.25.1
php7-tidy-7.2.5-lp151.6.25.1
php7-xmlrpc-7.2.5-lp151.6.25.1
php7-bz2-debuginfo-7.2.5-lp151.6.25.1
php7-curl-debuginfo-7.2.5-lp151.6.25.1
php7-fastcgi-7.2.5-lp151.6.25.1
php7-pcntl-7.2.5-lp151.6.25.1
php7-embed-debuginfo-7.2.5-lp151.6.25.1
php7-soap-7.2.5-lp151.6.25.1
php7-sodium-debuginfo-7.2.5-lp151.6.25.1
tidy-5.4.0-lp151.3.3.1
php7-opcache-7.2.5-lp151.6.25.1
php7-dom-7.2.5-lp151.6.25.1
php7-iconv-7.2.5-lp151.6.25.1
php7-sysvshm-debuginfo-7.2.5-lp151.6.25.1
php7-xmlreader-debuginfo-7.2.5-lp151.6.25.1
php7-ctype-7.2.5-lp151.6.25.1
php7-tokenizer-debuginfo-7.2.5-lp151.6.25.1
php7-json-7.2.5-lp151.6.25.1
php7-readline-debuginfo-7.2.5-lp151.6.25.1
php7-xmlreader-7.2.5-lp151.6.25.1
php7-enchant-7.2.5-lp151.6.25.1
php7-odbc-debuginfo-7.2.5-lp151.6.25.1
tidy-debuginfo-5.4.0-lp151.3.3.1
php7-sockets-7.2.5-lp151.6.25.1
php7-phar-debuginfo-7.2.5-lp151.6.25.1
php7-gmp-7.2.5-lp151.6.25.1

148971 - SuSE SLED 15 SP1, 15 SP2 SUSE-SU-2020:1225-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12393, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1225-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006810.html

SuSE SLED 15 SP1

x86_64
MozillaThunderbird-translations-other-68.8.0-3.80.2
MozillaThunderbird-translations-common-68.8.0-3.80.2
MozillaThunderbird-debuginfo-68.8.0-3.80.2
MozillaThunderbird-68.8.0-3.80.2
MozillaThunderbird-debugsource-68.8.0-3.80.2

SuSE SLED 15 SP2
x86_64
MozillaThunderbird-translations-other-68.8.0-3.80.2
MozillaThunderbird-translations-common-68.8.0-3.80.2
MozillaThunderbird-debuginfo-68.8.0-3.80.2
MozillaThunderbird-68.8.0-3.80.2
MozillaThunderbird-debugsource-68.8.0-3.80.2

148972 - SuSE SLES 12 SP4, 12 SP5 SUSE-SU-2020:1218-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12388, CVE-2020-12389, CVE-2020-12392, CVE-2020-12393, CVE-2020-12395, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1218-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006803.html

SuSE SLES 12 SP4
x86_64
MozillaFirefox-68.8.0-109.119.1
MozillaFirefox-translations-common-68.8.0-109.119.1
MozillaFirefox-debugsource-68.8.0-109.119.1
MozillaFirefox-debuginfo-68.8.0-109.119.1

SuSE SLES 12 SP5
x86_64
MozillaFirefox-68.8.0-109.119.1
MozillaFirefox-translations-common-68.8.0-109.119.1
MozillaFirefox-debugsource-68.8.0-109.119.1
MozillaFirefox-debuginfo-68.8.0-109.119.1

148973 - SuSE SLES 12 SP4, 12 SP5 SUSE-SU-2020:1272-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1927, CVE-2020-1934, CVE-2020-1938

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1272-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006814.html

SuSE SLES 12 SP4
noarch
apache2-doc-2.4.23-29.54.1

x86_64
apache2-prefork-debuginfo-2.4.23-29.54.1
apache2-2.4.23-29.54.1
apache2-utils-2.4.23-29.54.1
apache2-prefork-2.4.23-29.54.1
apache2-debuginfo-2.4.23-29.54.1
apache2-example-pages-2.4.23-29.54.1
apache2-debugsource-2.4.23-29.54.1
apache2-worker-debuginfo-2.4.23-29.54.1
apache2-worker-2.4.23-29.54.1
apache2-utils-debuginfo-2.4.23-29.54.1

SuSE SLES 12 SP5
noarch
apache2-doc-2.4.23-29.54.1

x86_64
apache2-prefork-debuginfo-2.4.23-29.54.1
apache2-2.4.23-29.54.1
apache2-utils-2.4.23-29.54.1
apache2-prefork-2.4.23-29.54.1
apache2-debuginfo-2.4.23-29.54.1
apache2-example-pages-2.4.23-29.54.1
apache2-debugsource-2.4.23-29.54.1
apache2-worker-debuginfo-2.4.23-29.54.1
apache2-worker-2.4.23-29.54.1
apache2-utils-debuginfo-2.4.23-29.54.1

148974 - SuSE Linux 15.1 openSUSE-SU-2020:0624-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-15681, CVE-2019-15690, CVE-2019-20788

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0624-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00079.html

SuSE Linux 15.1
x86_64
libvncclient0-debuginfo-0.9.10-lp151.7.3.1
libvncserver0-debuginfo-0.9.10-lp151.7.3.1

LibVNCServer-debugsource-0.9.10-lp151.7.3.1
libvncserver0-0.9.10-lp151.7.3.1
LibVNCServer-devel-0.9.10-lp151.7.3.1
libvncclient0-0.9.10-lp151.7.3.1

i586
libvncclient0-debuginfo-0.9.10-lp151.7.3.1
libvncserver0-debuginfo-0.9.10-lp151.7.3.1
LibVNCServer-debugsource-0.9.10-lp151.7.3.1
libvncserver0-0.9.10-lp151.7.3.1
LibVNCServer-devel-0.9.10-lp151.7.3.1
libvncclient0-0.9.10-lp151.7.3.1

148975 - SuSE Linux 15.1 openSUSE-SU-2020:0627-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-5267

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0627-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00062.html

SuSE Linux 15.1
x86_64
ruby2.5-rubygem-actionview-doc-5_1-5.1.4-lp151.3.3.1
ruby2.5-rubygem-actionview-5_1-5.1.4-lp151.3.3.1

148976 - SuSE SLED 12 SP4, 12 SP5 SUSE-SU-2020:1264-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12105

Description

The scan detected that the host is missing the following update:
SUSE-SU-2020:1264-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2020-May/006813.html

SuSE SLED 12 SP4
x86_64
openconnect-debuginfo-7.08-3.9.1
openconnect-7.08-3.9.1
openconnect-debugsource-7.08-3.9.1

noarch
openconnect-lang-7.08-3.9.1

SuSE SLED 12 SP5
x86_64
openconnect-debuginfo-7.08-3.9.1
openconnect-7.08-3.9.1
openconnect-debugsource-7.08-3.9.1

noarch
openconnect-lang-7.08-3.9.1

148977 - SuSE Linux 15.1 openSUSE-SU-2020:0621-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-12387, CVE-2020-12388, CVE-2020-12389, CVE-2020-12392, CVE-2020-12393, CVE-2020-12395, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0621-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2020-05/msg00064.html

SuSE Linux 15.1
x86_64
MozillaFirefox-buildsymbols-68.8.0-lp151.2.45.1
MozillaFirefox-translations-other-68.8.0-lp151.2.45.1
MozillaFirefox-68.8.0-lp151.2.45.1
MozillaFirefox-debugsource-68.8.0-lp151.2.45.1
MozillaFirefox-branding-upstream-68.8.0-lp151.2.45.1
MozillaFirefox-debuginfo-68.8.0-lp151.2.45.1
MozillaFirefox-translations-common-68.8.0-lp151.2.45.1
MozillaFirefox-devel-68.8.0-lp151.2.45.1

164207 - Oracle Enterprise Linux ELSA-2020-2070 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1763

Description

The scan detected that the host is missing the following update:
ELSA-2020-2070

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009911.html

OEL8
x86_64
libreswan-3.29-7.0.1.el8_2

164209 - Oracle Enterprise Linux ELSA-2020-2040 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-12519, CVE-2019-12525, CVE-2020-11945

Description

The scan detected that the host is missing the following update:
ELSA-2020-2040

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009890.html

OEL7
x86_64
squid-3.5.20-15.el7_8.1
squid-sysvinit-3.5.20-15.el7_8.1
squid-migration-script-3.5.20-15.el7_8.1

164210 - Oracle Enterprise Linux ELSA-2020-2082 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18595, CVE-2019-19768, CVE-2020-10711

Description

The scan detected that the host is missing the following update:
ELSA-2020-2082

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009926.html

OEL7
x86_64
kernel-tools-libs-devel-3.10.0-1127.8.2.el7
kernel-3.10.0-1127.8.2.el7
kernel-abi-whitelists-3.10.0-1127.8.2.el7
kernel-debug-devel-3.10.0-1127.8.2.el7
kernel-doc-3.10.0-1127.8.2.el7
perf-3.10.0-1127.8.2.el7
bpftool-3.10.0-1127.8.2.el7
python-perf-3.10.0-1127.8.2.el7
kernel-tools-3.10.0-1127.8.2.el7
kernel-devel-3.10.0-1127.8.2.el7
kernel-tools-libs-3.10.0-1127.8.2.el7
kernel-headers-3.10.0-1127.8.2.el7

kernel-debug-3.10.0-1127.8.2.el7

164212 - Oracle Enterprise Linux ELSA-2020-1926 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-14378, CVE-2019-9512, CVE-2019-9514, CVE-2020-10696, CVE-2020-7039

Description

The scan detected that the host is missing the following update:
ELSA-2020-1926

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009920.html

OEL8
x86_64
crit-3.12-9.module+el8.2.0+7621+b33f33e5
podman-1.0.0-4.git921f98f.module+el8.2.0+7621+b33f33e5
oci-systemd-hook-0.1.15-2.git2d0b8a3.module+el8.2.0+7621+b33f33e5
buildah-1.5-4.0.1.gite94b4f9.module+el8.2.0+7621+b33f33e5
criu-3.12-9.module+el8.2.0+7621+b33f33e5
skopeo-0.1.32-4.0.2.git1715c90.module+el8.2.0+7621+b33f33e5
containers-common-0.1.32-4.0.2.git1715c90.module+el8.2.0+7621+b33f33e5
podman-docker-1.0.0-4.git921f98f.module+el8.2.0+7621+b33f33e5
containernetworking-plugins-0.7.4-3.git9ebe139.module+el8.2.0+7621+b33f33e5
fuse-overlayfs-0.3-5.module+el8.2.0+7621+b33f33e5
container-selinux-2.124.0-1.gitf958d0c.module+el8.2.0+7621+b33f33e5
python3-criu-3.12-9.module+el8.2.0+7621+b33f33e5
runc-1.0.0-56.rc5.dev.git2abd837.module+el8.2.0+7621+b33f33e5
oci-umount-2.3.4-2.git87f9237.module+el8.2.0+7621+b33f33e5
slirp4netns-0.1-5.dev.gitc4e1bc5.module+el8.2.0+7621+b33f33e5

164213 - Oracle Enterprise Linux ELSA-2020-2103 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10711

Description

The scan detected that the host is missing the following update:
ELSA-2020-2103

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009918.html

OEL6
x86_64
kernel-doc-2.6.32-754.29.2.el6
kernel-firmware-2.6.32-754.29.2.el6

kernel-headers-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
python-perf-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-abi-whitelists-2.6.32-754.29.2.el6
kernel-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6

i386
kernel-doc-2.6.32-754.29.2.el6
kernel-firmware-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
python-perf-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-abi-whitelists-2.6.32-754.29.2.el6
kernel-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6

164214 - Oracle Enterprise Linux ELSA-2020-2143 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1108

Description

The scan detected that the host is missing the following update:
ELSA-2020-2143

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009922.html

OEL8
x86_64
dotnet-sdk-2.1.5xx-2.1.514-2.el8_2
dotnet-host-fxr-2.1-2.1.18-2.el8_2
dotnet-runtime-2.1-2.1.18-2.el8_2
dotnet-sdk-2.1-2.1.514-2.el8_2

164216 - Oracle Enterprise Linux ELSA-2020-1980 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-11008

Description

The scan detected that the host is missing the following update:
ELSA-2020-1980

Observation

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

For more information see:

http://oss.oracle.com/pipermail/el-errata/2020-May/009896.html

OEL8
x86_64
gitk-2.18.4-2.el8_2
git-instaweb-2.18.4-2.el8_2
perl-Git-2.18.4-2.el8_2
perl-Git-SVN-2.18.4-2.el8_2
git-core-doc-2.18.4-2.el8_2
git-all-2.18.4-2.el8_2
git-2.18.4-2.el8_2
git-subtree-2.18.4-2.el8_2
git-daemon-2.18.4-2.el8_2
git-svn-2.18.4-2.el8_2
git-email-2.18.4-2.el8_2
git-gui-2.18.4-2.el8_2
gitweb-2.18.4-2.el8_2
git-core-2.18.4-2.el8_2

164218 - Oracle Enterprise Linux ELSA-2020-2041 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-12519, CVE-2019-12525, CVE-2020-11945

Description

The scan detected that the host is missing the following update:
ELSA-2020-2041

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009910.html

OEL8
x86_64
libecap-1.0.1-2.module+el8.1.0+5405+03b963f4
squid-4.4-8.module+el8.2.0+7611+d512f060.1
libecap-devel-1.0.1-2.module+el8.1.0+5405+03b963f4

164221 - Oracle Enterprise Linux ELSA-2020-1932 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-19921, CVE-2020-10696

Description

The scan detected that the host is missing the following update:
ELSA-2020-1932

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009917.html

OEL8
x86_64
runc-1.0.0-65.rc10.module+el8.2.0+7615+180dc822
podman-tests-1.6.4-11.0.1.module+el8.2.0+7615+180dc822
podman-remote-1.6.4-11.0.1.module+el8.2.0+7615+180dc822
podman-docker-1.6.4-11.0.1.module+el8.2.0+7615+180dc822
skopeo-0.1.40-11.0.1.module+el8.2.0+7615+180dc822
container-selinux-2.124.0-1.module+el8.2.0+7615+180dc822
podman-1.6.4-11.0.1.module+el8.2.0+7615+180dc822
python3-criu-3.12-9.module+el8.2.0+7615+180dc822
udica-0.2.1-2.module+el8.2.0+7615+180dc822
criu-3.12-9.module+el8.2.0+7615+180dc822
fuse-overlayfs-0.7.2-5.module+el8.2.0+7615+180dc822
crit-3.12-9.module+el8.2.0+7615+180dc822
containers-common-0.1.40-11.0.1.module+el8.2.0+7615+180dc822
cockpit-podman-12-1.module+el8.2.0+7615+180dc822
skopeo-tests-0.1.40-11.0.1.module+el8.2.0+7615+180dc822
containernetworking-plugins-0.8.3-5.0.1.module+el8.2.0+7615+180dc822
buildah-1.11.6-8.0.1.module+el8.2.0+7615+180dc822
slirp4netns-0.4.2-3.git21fdece.module+el8.2.0+7615+180dc822
python-podman-api-1.2.0-0.2.gitd0a45fe.module+el8.2.0+7615+180dc822
conmon-2.0.6-1.0.1.module+el8.2.0+7615+180dc822
buildah-tests-1.11.6-8.0.1.module+el8.2.0+7615+180dc822

164222 - Oracle Enterprise Linux ELSA-2020-2102 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10711, CVE-2020-11884, CVE-2020-2732

Description

The scan detected that the host is missing the following update:
ELSA-2020-2102

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009921.html

OEL8
x86_64
kernel-tools-4.18.0-193.1.2.el8_2
kernel-abi-whitelists-4.18.0-193.1.2.el8_2
perf-4.18.0-193.1.2.el8_2
kernel-headers-4.18.0-193.1.2.el8_2
kernel-devel-4.18.0-193.1.2.el8_2
kernel-tools-libs-4.18.0-193.1.2.el8_2
kernel-modules-4.18.0-193.1.2.el8_2
bpftool-4.18.0-193.1.2.el8_2
kernel-debug-modules-4.18.0-193.1.2.el8_2
kernel-debug-devel-4.18.0-193.1.2.el8_2
kernel-core-4.18.0-193.1.2.el8_2
python3-perf-4.18.0-193.1.2.el8_2
kernel-doc-4.18.0-193.1.2.el8_2

kernel-4.18.0-193.1.2.el8_2
kernel-debug-4.18.0-193.1.2.el8_2
kernel-modules-extra-4.18.0-193.1.2.el8_2
kernel-debug-modules-extra-4.18.0-193.1.2.el8_2
kernel-tools-libs-devel-4.18.0-193.1.2.el8_2
kernel-debug-core-4.18.0-193.1.2.el8_2
kernel-cross-headers-4.18.0-193.1.2.el8_2

164223 - Oracle Enterprise Linux ELSA-2020-1933 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10699

Description

The scan detected that the host is missing the following update:
ELSA-2020-1933

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009895.html

OEL8
x86_64
targetcli-2.1.51-4.el8_2

164225 - Oracle Enterprise Linux ELSA-2020-1931 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10696

Description

The scan detected that the host is missing the following update:
ELSA-2020-1931

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009915.html

OEL8
x86_64
python-podman-api-1.2.0-0.2.gitd0a45fe.module+el8.2.0+7618+3a616245
slirp4netns-0.4.2-3.git21fdece.module+el8.2.0+7618+3a616245
criu-3.12-9.module+el8.2.0+7618+3a616245
runc-1.0.0-64.rc10.module+el8.2.0+7618+3a616245
cockpit-podman-11-1.module+el8.2.0+7618+3a616245
crit-3.12-9.module+el8.2.0+7618+3a616245
fuse-overlayfs-0.7.2-5.module+el8.2.0+7618+3a616245
skopeo-tests-0.1.40-9.0.1.module+el8.2.0+7618+3a616245
podman-1.6.4-11.0.1.module+el8.2.0+7618+3a616245
python3-criu-3.12-9.module+el8.2.0+7618+3a616245

conmon-2.0.6-1.0.1.module+el8.2.0+7618+3a616245
skopeo-0.1.40-9.0.1.module+el8.2.0+7618+3a616245
containers-common-0.1.40-9.0.1.module+el8.2.0+7618+3a616245
podman-tests-1.6.4-11.0.1.module+el8.2.0+7618+3a616245
containernetworking-plugins-0.8.3-4.0.1.module+el8.2.0+7618+3a616245
podman-remote-1.6.4-11.0.1.module+el8.2.0+7618+3a616245
container-selinux-2.124.0-1.module+el8.2.0+7618+3a616245
buildah-1.11.6-7.0.1.module+el8.2.0+7618+3a616245
udica-0.2.1-2.module+el8.2.0+7618+3a616245
podman-docker-1.6.4-11.0.1.module+el8.2.0+7618+3a616245
buildah-tests-1.11.6-7.0.1.module+el8.2.0+7618+3a616245

171215 - Amazon Linux AMI ALAS-2020-1366 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10711

Description

The scan detected that the host is missing the following update:
ALAS-2020-1366

Observation

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

https://alas.aws.amazon.com/ALAS-2020-1366.html

Amazon Linux AMI
x86_64
kernel-debuginfo-common-x86_64-4.14.177-107.254.amzn1
kernel-tools-devel-4.14.177-107.254.amzn1
kernel-debuginfo-4.14.177-107.254.amzn1
kernel-4.14.177-107.254.amzn1
kernel-tools-4.14.177-107.254.amzn1
kernel-headers-4.14.177-107.254.amzn1
kernel-tools-debuginfo-4.14.177-107.254.amzn1
perf-4.14.177-107.254.amzn1
kernel-devel-4.14.177-107.254.amzn1
perf-debuginfo-4.14.177-107.254.amzn1

i686
perf-debuginfo-4.14.177-107.254.amzn1
kernel-tools-devel-4.14.177-107.254.amzn1
kernel-debuginfo-4.14.177-107.254.amzn1
kernel-debuginfo-common-i686-4.14.177-107.254.amzn1
kernel-tools-4.14.177-107.254.amzn1
kernel-headers-4.14.177-107.254.amzn1
kernel-tools-debuginfo-4.14.177-107.254.amzn1
perf-4.14.177-107.254.amzn1
kernel-devel-4.14.177-107.254.amzn1
kernel-4.14.177-107.254.amzn1

171216 - Amazon Linux AMI ALAS-2020-1365 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-2756, CVE-2020-2757, CVE-2020-2773, CVE-2020-2781, CVE-2020-2800, CVE-2020-2803, CVE-2020-2805, CVE-2020-2830

Description

The scan detected that the host is missing the following update:
ALAS-2020-1365

Observation

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

https://alas.aws.amazon.com/ALAS-2020-1365.html

Amazon Linux AMI
i686
java-1.7.0-openjdk-demo-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-devel-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-src-1.7.0.261-2.6.22.1.83.amzn1

noarch
java-1.7.0-openjdk-javadoc-1.7.0.261-2.6.22.1.83.amzn1

x86_64
java-1.7.0-openjdk-devel-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-demo-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-src-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-1.7.0.261-2.6.22.1.83.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.261-2.6.22.1.83.amzn1

171217 - Amazon Linux AMI ALAS-2020-1364 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2716

Description

The scan detected that the host is missing the following update:
ALAS-2020-1364

Observation

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

https://alas.aws.amazon.com/ALAS-2020-1364.html

Amazon Linux AMI
x86_64
expat-debuginfo-2.1.0-11.22.amzn1
expat-2.1.0-11.22.amzn1
expat-devel-2.1.0-11.22.amzn1

i686
expat-debuginfo-2.1.0-11.22.amzn1
expat-devel-2.1.0-11.22.amzn1
expat-2.1.0-11.22.amzn1

171219 - Amazon Linux AMI ALAS-2020-1363 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3814, CVE-2019-7524

Description

The scan detected that the host is missing the following update:
ALAS-2020-1363

Observation

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

https://alas.aws.amazon.com/ALAS-2020-1363.html

Amazon Linux AMI
x86_64
dovecot-debuginfo-2.2.36-6.19.amzn1
dovecot-pigeonhole-2.2.36-6.19.amzn1
dovecot-devel-2.2.36-6.19.amzn1
dovecot-mysql-2.2.36-6.19.amzn1
dovecot-2.2.36-6.19.amzn1
dovecot-pgsql-2.2.36-6.19.amzn1

i686
dovecot-devel-2.2.36-6.19.amzn1
dovecot-pigeonhole-2.2.36-6.19.amzn1
dovecot-debuginfo-2.2.36-6.19.amzn1
dovecot-mysql-2.2.36-6.19.amzn1
dovecot-2.2.36-6.19.amzn1
dovecot-pgsql-2.2.36-6.19.amzn1

178861 - Gentoo Linux GLSA-202005-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-202005-05

Observation

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

https://security.gentoo.org/glsa/202005-05

Affected packages:
net-proxy/squid < 4.11

196725 - Red Hat Enterprise Linux RHSA-2020-2103 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-10711

Description

The scan detected that the host is missing the following update:
RHSA-2020-2103

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00036.html

RHEL6D
i386
perf-debuginfo-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
kernel-debuginfo-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
python-perf-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-debuginfo-common-i686-2.6.32-754.29.2.el6
kernel-debug-debuginfo-2.6.32-754.29.2.el6
kernel-2.6.32-754.29.2.el6
python-perf-debuginfo-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6

noarch
kernel-doc-2.6.32-754.29.2.el6
kernel-abi-whitelists-2.6.32-754.29.2.el6
kernel-firmware-2.6.32-754.29.2.el6

x86_64
kernel-2.6.32-754.29.2.el6
kernel-debuginfo-2.6.32-754.29.2.el6
kernel-debuginfo-common-i686-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6
kernel-debuginfo-common-x86_64-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
python-perf-2.6.32-754.29.2.el6
kernel-debug-debuginfo-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
python-perf-debuginfo-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
perf-debuginfo-2.6.32-754.29.2.el6

RHEL6S
i386
perf-debuginfo-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
kernel-debuginfo-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
python-perf-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-debuginfo-common-i686-2.6.32-754.29.2.el6
kernel-debug-debuginfo-2.6.32-754.29.2.el6
kernel-2.6.32-754.29.2.el6

python-perf-debuginfo-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6

noarch
kernel-doc-2.6.32-754.29.2.el6
kernel-abi-whitelists-2.6.32-754.29.2.el6
kernel-firmware-2.6.32-754.29.2.el6

x86_64
kernel-2.6.32-754.29.2.el6
kernel-debuginfo-2.6.32-754.29.2.el6
kernel-debuginfo-common-i686-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6
kernel-debuginfo-common-x86_64-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
python-perf-2.6.32-754.29.2.el6
kernel-debug-debuginfo-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
python-perf-debuginfo-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
perf-debuginfo-2.6.32-754.29.2.el6

RHEL6WS
i386
perf-debuginfo-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
kernel-debuginfo-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-debuginfo-common-i686-2.6.32-754.29.2.el6
kernel-debug-debuginfo-2.6.32-754.29.2.el6
kernel-2.6.32-754.29.2.el6
python-perf-debuginfo-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6

noarch
kernel-doc-2.6.32-754.29.2.el6
kernel-abi-whitelists-2.6.32-754.29.2.el6
kernel-firmware-2.6.32-754.29.2.el6

x86_64
perf-debuginfo-2.6.32-754.29.2.el6
kernel-headers-2.6.32-754.29.2.el6
kernel-debuginfo-2.6.32-754.29.2.el6
kernel-debug-2.6.32-754.29.2.el6
python-perf-debuginfo-2.6.32-754.29.2.el6
kernel-devel-2.6.32-754.29.2.el6
kernel-debuginfo-common-i686-2.6.32-754.29.2.el6
kernel-debug-debuginfo-2.6.32-754.29.2.el6
kernel-2.6.32-754.29.2.el6
perf-2.6.32-754.29.2.el6
kernel-debuginfo-common-x86_64-2.6.32-754.29.2.el6
kernel-debug-devel-2.6.32-754.29.2.el6

196727 - Red Hat Enterprise Linux RHSA-2020-2082 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18595, CVE-2019-19768, CVE-2020-10711

Description

The scan detected that the host is missing the following update:
RHSA-2020-2082

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00044.html

RHEL7D
x86_64
python-perf-debuginfo-3.10.0-1127.8.2.el7
kernel-tools-libs-devel-3.10.0-1127.8.2.el7
kernel-3.10.0-1127.8.2.el7
kernel-tools-debuginfo-3.10.0-1127.8.2.el7
kernel-debug-devel-3.10.0-1127.8.2.el7
perf-3.10.0-1127.8.2.el7
bpftool-debuginfo-3.10.0-1127.8.2.el7
kernel-debug-debuginfo-3.10.0-1127.8.2.el7
perf-debuginfo-3.10.0-1127.8.2.el7
bpftool-3.10.0-1127.8.2.el7
python-perf-3.10.0-1127.8.2.el7
kernel-tools-3.10.0-1127.8.2.el7
kernel-debuginfo-common-x86_64-3.10.0-1127.8.2.el7
kernel-debuginfo-3.10.0-1127.8.2.el7
kernel-devel-3.10.0-1127.8.2.el7
kernel-tools-libs-3.10.0-1127.8.2.el7
kernel-headers-3.10.0-1127.8.2.el7
kernel-debug-3.10.0-1127.8.2.el7

noarch
kernel-doc-3.10.0-1127.8.2.el7
kernel-abi-whitelists-3.10.0-1127.8.2.el7

RHEL7S
noarch
kernel-doc-3.10.0-1127.8.2.el7
kernel-abi-whitelists-3.10.0-1127.8.2.el7

x86_64
python-perf-debuginfo-3.10.0-1127.8.2.el7
kernel-tools-libs-devel-3.10.0-1127.8.2.el7
kernel-3.10.0-1127.8.2.el7
kernel-tools-debuginfo-3.10.0-1127.8.2.el7
kernel-debug-devel-3.10.0-1127.8.2.el7
perf-3.10.0-1127.8.2.el7
bpftool-debuginfo-3.10.0-1127.8.2.el7
kernel-debug-debuginfo-3.10.0-1127.8.2.el7
perf-debuginfo-3.10.0-1127.8.2.el7
bpftool-3.10.0-1127.8.2.el7
python-perf-3.10.0-1127.8.2.el7
kernel-tools-3.10.0-1127.8.2.el7
kernel-debuginfo-common-x86_64-3.10.0-1127.8.2.el7
kernel-debuginfo-3.10.0-1127.8.2.el7
kernel-devel-3.10.0-1127.8.2.el7

kernel-tools-libs-3.10.0-1127.8.2.el7
kernel-headers-3.10.0-1127.8.2.el7
kernel-debug-3.10.0-1127.8.2.el7

RHEL7WS
x86_64
python-perf-debuginfo-3.10.0-1127.8.2.el7
kernel-tools-libs-devel-3.10.0-1127.8.2.el7
kernel-3.10.0-1127.8.2.el7
kernel-tools-debuginfo-3.10.0-1127.8.2.el7
kernel-debug-devel-3.10.0-1127.8.2.el7
perf-3.10.0-1127.8.2.el7
bpftool-debuginfo-3.10.0-1127.8.2.el7
kernel-debug-debuginfo-3.10.0-1127.8.2.el7
perf-debuginfo-3.10.0-1127.8.2.el7
bpftool-3.10.0-1127.8.2.el7
python-perf-3.10.0-1127.8.2.el7
kernel-tools-3.10.0-1127.8.2.el7
kernel-debuginfo-common-x86_64-3.10.0-1127.8.2.el7
kernel-debuginfo-3.10.0-1127.8.2.el7
kernel-devel-3.10.0-1127.8.2.el7
kernel-tools-libs-3.10.0-1127.8.2.el7
kernel-headers-3.10.0-1127.8.2.el7
kernel-debug-3.10.0-1127.8.2.el7

noarch
kernel-doc-3.10.0-1127.8.2.el7
kernel-abi-whitelists-3.10.0-1127.8.2.el7

196729 - Red Hat Enterprise Linux RHSA-2020-2040 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-12519, CVE-2019-12525, CVE-2020-11945

Description

The scan detected that the host is missing the following update:
RHSA-2020-2040

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00015.html

RHEL7S
x86_64
squid-3.5.20-15.el7_8.1
squid-sysvinit-3.5.20-15.el7_8.1
squid-debuginfo-3.5.20-15.el7_8.1
squid-migration-script-3.5.20-15.el7_8.1

RHEL7WS
x86_64
squid-3.5.20-15.el7_8.1
squid-sysvinit-3.5.20-15.el7_8.1
squid-debuginfo-3.5.20-15.el7_8.1
squid-migration-script-3.5.20-15.el7_8.1

196731 - Red Hat Enterprise Linux RHSA-2020-2064 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-6464, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
RHSA-2020-2064

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00028.html

RHEL6D
i386
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

i686
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

x86_64
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

RHEL6S
i386
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

i686
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

x86_64
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

RHEL6WS
i386
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

i686
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

x86_64
chromium-browser-81.0.4044.138-1.el6_10
chromium-browser-debuginfo-81.0.4044.138-1.el6_10

26425 - (MSPT-May2020) Microsoft Windows Kernel-Mode Driver Privilege Escalation (CVE-2020-1143)

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

Risk Level: Medium

CVE: CVE-2020-1143

Description

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

Observation

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

The flaw lies in the Kernel-Mode Driver 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.

26432 - (MSPT-May2020) Microsoft Windows Error Reporting Privilege Escalation (CVE-2020-1132)

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

Risk Level: Medium

CVE: CVE-2020-1132

Description

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

Observation

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

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

26484 - (MSPT-May2020) Microsoft Windows Media Foundation Memory Corruption Vulnerability (CVE-2020-1126)

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

Risk Level: Medium

CVE: CVE-2020-1126

Description

A vulnerability in some versions of Microsoft Windows could lead to Memory Corruption.

Observation

A vulnerability in some versions of Microsoft Windows could lead to Memory Corruption.

The flaw lies in the Media Foundation component. Successful exploitation by a remote attacker could result in Secuirty Bypass. The exploit requires the user to open a vulnerable website, email or document.

26493 - (MSPT-May2020) Microsoft Edge Improperly Enforce Cross-Domain Policies Privilege Escalation (CVE-2020-1056)

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

Risk Level: Medium

CVE: CVE-2020-1056

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 improperly enforce cross-domain policies. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

26509 - (MSPT-May2020) Microsoft Windows Kernel-Mode Privilege Escalation (CVE-2020-1054)

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

Risk Level: Medium

CVE: CVE-2020-1054

Description

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

Observation

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

The flaw lies in the Kernel-Mode 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.

26518 - (MSPT-May2020) Microsoft Windows SharePoint Information Disclosure (CVE-2020-1103)

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

Risk Level: Medium

CVE: CVE-2020-1103

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 SharePoint 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.

26519 - (MSPT-May2020) Microsoft Windows SharePoint Spoofing (CVE-2020-1104)

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

Risk Level: Medium

CVE: CVE-2020-1104

Description

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

Observation

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

The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in spoofing

26521 - (MSPT-May2020) Microsoft SharePoint Cross Site Scripting Vulnerability (CVE-2020-1106)

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

Risk Level: Medium

CVE: CVE-2020-1106

Description

A vulnerability in some versions of Microsoft SharePoint could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to spoofing.

The flaw lies in improperly sanitize crafted web request. Successful exploitation by a remote attacker could result in spoofing

26522 - (MSPT-May2020) Microsoft SharePoint Improperly Sanitize Crafted Web Request Spoofing (CVE-2020-1107)

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

Risk Level: Medium

CVE: CVE-2020-1107

Description

A vulnerability in some versions of Microsoft SharePoint could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to spoofing.

The flaw lies in improperly sanitize crafted web request. Successful exploitation by a remote attacker could result in spoofing

131585 - Debian Linux 10.0, 9.0 DSA-4677-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-16217, CVE-2019-16218, CVE-2019-16219, CVE-2019-16220, CVE-2019-16221, CVE-2019-16222, CVE-2019-16223, CVE-2019-16780, CVE-2019-16781, CVE-2019-17669, CVE-2019-17671, CVE-2019-17672, CVE-2019-17673, CVE-2019-17674, CVE-2019-17675, CVE-2019-20041, CVE-2019-20042, CVE-2019-20043, CVE-2019-9787, CVE-2020-11025, CVE-2020-11026, CVE-2020-11027, CVE-2020-11028, CVE-2020-11029, CVE-2020-11030

Description

The scan detected that the host is missing the following update:
DSA-4677-1

Observation

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

http://www.debian.org/security/2020/dsa-4677

Debian 9.0
all
wordpress_4.7.5+dfsg-2+deb9u6

Debian 10.0
all
wordpress_5.0.4+dfsg1-1+deb10u2

164215 - Oracle Enterprise Linux ELSA-2020-5676 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1798, CVE-2018-19854, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, CVE-2019-19462, CVE-2019-19527, CVE-2019-19532, CVE-2019-19768, CVE-2019-19965, CVE-2019-20096, CVE-2020-11494, CVE-2020-8647, CVE-2020-8648, CVE-2020-8649, CVE-2020-9383

Description

The scan detected that the host is missing the following update:
ELSA-2020-5676

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009907.html

OEL7
x86_64
kernel-uek-debug-devel-4.14.35-1902.302.2.el7uek
kernel-uek-4.14.35-1902.302.2.el7uek
kernel-uek-debug-4.14.35-1902.302.2.el7uek
kernel-uek-devel-4.14.35-1902.302.2.el7uek
kernel-uek-tools-4.14.35-1902.302.2.el7uek
kernel-uek-doc-4.14.35-1902.302.2.el7uek

26424 - (MSPT-May2020) Microsoft Windows Kernel Information Disclosure (CVE-2020-1072)

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

Risk Level: Medium

CVE: CVE-2020-1072

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 Kernel 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.

26430 - (MSPT-May2020) Microsoft WER Improperly Handles and Executes Files Privilege Escalation (CVE-2020-1082)

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

Risk Level: Medium

CVE: CVE-2020-1082

Description

A vulnerability in some versions of Microsoft windows error reporting could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft windows error reporting could lead to privilege escalation.

The flaw lies in improperly handles and executes files. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26435 - (MSPT-May2020) Microsoft Windows Printer Service Privilege Escalation (CVE-2020-1081)

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

Risk Level: Medium

CVE: CVE-2020-1081

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 Printer Service 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.

26436 - (MSPT-May2020) Microsoft Windows Print Spooler Privilege Escalation (CVE-2020-1070)

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

Risk Level: Medium

CVE: CVE-2020-1070

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 Print Spooler 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.

26437 - (MSPT-May2020) Microsoft Windows Print Spooler Privilege Escalation (CVE-2020-1048)

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

Risk Level: Medium

CVE: CVE-2020-1048

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 Print Spooler 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.

26438 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1077)

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

Risk Level: Medium

CVE: CVE-2020-1077

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 Runtime 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.

26439 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1086)

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

Risk Level: Medium

CVE: CVE-2020-1086

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 Runtime 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.

26440 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1125)

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

Risk Level: Medium

CVE: CVE-2020-1125

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 Runtime 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.

26441 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1139)

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

Risk Level: Medium

CVE: CVE-2020-1139

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 Runtime 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.

26442 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1090)

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

Risk Level: Medium

CVE: CVE-2020-1090

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 Runtime 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.

26443 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1149)

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

Risk Level: Medium

CVE: CVE-2020-1149

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 Runtime 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.

26444 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1155)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2020-1155

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 Runtime 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.

26445 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1156)

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

Risk Level: Medium

CVE: CVE-2020-1156

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 Runtime 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.

26446 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1124)

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

Risk Level: Medium

CVE: CVE-2020-1124

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 State Repository Service 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.

26447 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1144)

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

Risk Level: Medium

CVE: CVE-2020-1144

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 State Repository Service 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.

26448 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1134)

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

Risk Level: Medium

CVE: CVE-2020-1134

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 State Repository Service 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.

26449 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1131)

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

Risk Level: Medium

CVE: CVE-2020-1131

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 State Repository Service 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.

26450 - (MSPT-May2020) Microsoft Windows Subsystem for Linux Information Disclosure (CVE-2020-1075)

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

Risk Level: Medium

CVE: CVE-2020-1075

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 Subsystem for Linux 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.

26451 - (MSPT-May2020) Microsoft Windows Push Notification Service Privilege Escalation (CVE-2020-1164)

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

Risk Level: Medium

CVE: CVE-2020-1164

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 Push Notification Service 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.

26452 - (MSPT-May2020) Microsoft Windows Push Notification Service Privilege Escalation (CVE-2020-1137)

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

Risk Level: Medium

CVE: CVE-2020-1137

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 Push Notification Service 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.

26453 - (MSPT-May2020) Microsoft Windows Update Stack Privilege Escalation (CVE-2020-1109)

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

Risk Level: Medium

CVE: CVE-2020-1109

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 Update Stack 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.

26454 - (MSPT-May2020) Microsoft Windows Update Stack Privilege Escalation (CVE-2020-1110)

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

Risk Level: Medium

CVE: CVE-2020-1110

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 Update Stack 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.

26457 - (MSPT-May2020) Microsoft Windows NTLM password Privilege Escalation (CVE-2020-1113)

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

Risk Level: Medium

CVE: CVE-2020-1113

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 NTLM password 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.

26458 - (MSPT-May2020) Microsoft Windows BITS IIS module Privilege Escalation (CVE-2020-1112)

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

Risk Level: Medium

CVE: CVE-2020-1112

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 BITS IIS module. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26461 - (MSPT-May2020) Microsoft ADFS Improperly Sanitize User Inputs Spoofing (CVE-2020-1055)

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

Risk Level: Medium

CVE: CVE-2020-1055

Description

A vulnerability in some versions of Microsoft ADFS could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft ADFS could lead to spoofing.

The flaw lies in improperly sanitize user inputs. Successful exploitation by a remote attacker could result in spoofing

26473 - (MSPT-May2020) Microsoft Windows Power BI Report Server Spoofing (CVE-2020-1173)

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

Risk Level: Medium

CVE: CVE-2020-1173

Description

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

Observation

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

The flaw lies in the Power BI Report Server component. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

26478 - (MSPT-May2020) Microsoft Windows Wbengine Privilege Escalation (CVE-2020-1010)

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

Risk Level: Medium

CVE: CVE-2020-1010

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 Wbengine 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.

26479 - (MSPT-May2020) Microsoft Windows Media Foundation Memory Corruption Vulnerability (CVE-2020-1028)

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

Risk Level: Medium

CVE: CVE-2020-1028

Description

A vulnerability in some versions of Microsoft Windows could lead to memory corruption.

Observation

A vulnerability in some versions of Microsoft Windows could lead to memory corruption.

The flaw lies in the Media Foundation component. Successful exploitation by a remote attacker could result in security bypass and affect the integrity. The exploit requires the user to open a vulnerable website, email or document.

26480 - (MSPT-May2020) Microsoft Windows Privilege Escalation (CVE-2020-1068)

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

Risk Level: Medium

CVE: CVE-2020-1068

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 Media Service 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.

26481 - (MSPT-May2020) Microsoft Windows Privilege Escalation (CVE-2020-1079)

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

Risk Level: Medium

CVE: CVE-2020-1079

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 improperly handles 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.

26482 - (MSPT-May2020) Microsoft Windows Clipboard Service Privilege Escalation (CVE-2020-1111)

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

Risk Level: Medium

CVE: CVE-2020-1111

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 Clipboard Service 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.

26483 - (MSPT-May2020) Microsoft Windows Clipboard Service Privilege Escalation (CVE-2020-1121)

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

Risk Level: Medium

CVE: CVE-2020-1121

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 Clipboard Service 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.

26485 - (MSPT-May2020) Microsoft Windows Media Foundation Memory Corruption Vulnerability (CVE-2020-1136)

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

Risk Level: Medium

CVE: CVE-2020-1136

Description

A vulnerability in some versions of Microsoft Windows could lead to Memory Corruption.

Observation

A vulnerability in some versions of Microsoft Windows could lead to Memory Corruption.

The flaw lies in the Media Foundation component. Successful exploitation by a remote attacker could result in Security Bypass. The exploit requires the user to open a vulnerable website, email or document.

26486 - (MSPT-May2020) Microsoft Windows Clipboard Service Privilege Escalation (CVE-2020-1165)

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

Risk Level: Medium

CVE: CVE-2020-1165

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 Clipboard Service 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.

26487 - (MSPT-May2020) Microsoft Windows Clipboard Service Privilege Escalation (CVE-2020-1166)

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

Risk Level: Medium

CVE: CVE-2020-1166

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 Clipboard Service 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.

26494 - (MSPT-May2020) Microsoft Edge Properly Parse HTTP Content Spoofing (CVE-2020-1059)

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

Risk Level: Medium

CVE: CVE-2020-1059

Description

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

Observation

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

The flaw lies in properly parse HTTP content. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

26497 - (MSPT-May2020) Microsoft Windows Remote Access Common Dialog Privilege Escalation (CVE-2020-1071)

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

Risk Level: Medium

CVE: CVE-2020-1071

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 Remote Access Common Dialog 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.

26498 - (MSPT-May2020) Microsoft Windows Installer Privilege Escalation (CVE-2020-1078)

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

Risk Level: Medium

CVE: CVE-2020-1078

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 Installer 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.

26500 - (MSPT-May2020) Microsoft Windows CSRSS Information Disclosure (CVE-2020-1116)

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

Risk Level: Medium

CVE: CVE-2020-1116

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 CSRSS component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26501 - (MSPT-May2020) Microsoft Windows TLS Denial of Service (CVE-2020-1118)

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

Risk Level: Medium

CVE: CVE-2020-1118

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 in the TLS component. Successful exploitation by a remote attacker could result in a denial of service condition.

26502 - (MSPT-May2020) Microsoft Windows Connected User Experiences and Telemetry Service Privilege Escalation (CVE-2020-1123)

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

Risk Level: Medium

CVE: CVE-2020-1123

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 Connected User Experiences and Telemetry Service 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.

26503 - (MSPT-May2020) Microsoft Windows Storage Service Privilege Escalation (CVE-2020-1138)

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

Risk Level: Medium

CVE: CVE-2020-1138

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 Storage Service 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.

26504 - (MSPT-May2020) Microsoft DirectX Privilege Escalation (CVE-2020-1140)

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

Risk Level: Medium

CVE: CVE-2020-1140

Description

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

Observation

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

The flaw lies in improperly handles 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.

26505 - (MSPT-May2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1151)

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

Risk Level: Medium

CVE: CVE-2020-1151

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 Runtime 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.

26507 - (MSPT-May2020) Microsoft Windows CLFS Privilege Escalation (CVE-2020-1154)

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

Risk Level: Medium

CVE: CVE-2020-1154

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 CLFS 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.

26514 - (MSPT-May2020) Microsoft SharePoint Cross Site Scripting Vulnerability (CVE-2020-1099)

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

Risk Level: Medium

CVE: CVE-2020-1099

Description

A vulnerability in some versions of Microsoft SharePoint could lead to Cross Site Scripting.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to Cross Site Scripting.

The flaw lies in improperly sanitize crafted web request. Successful exploitation by a remote attacker could result in Cross Site Scripting Attack.

26516 - (MSPT-May2020) Microsoft SharePoint Cross Sire Scripting Vulnerability (CVE-2020-1101)

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

Risk Level: Medium

CVE: CVE-2020-1101

Description

A vulnerability in some versions of Microsoft SharePoint could lead to Cross Site Scripting.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to Cross Site Scripting.

The flaw lies in improperly sanitize crafted web request. Successful exploitation by a remote attacker could result in Cross Site Scripting.

26523 - (MSPT-May2020) Microsoft Windows GDI Information Disclosure (CVE-2020-1141)

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

Risk Level: Medium

CVE: CVE-2020-1141

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 attacker to have valid credentials to the vulnerable system.

26524 - (MSPT-May2020) Microsoft Windows GDI Information Disclosure (CVE-2020-1179)

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

Risk Level: Medium

CVE: CVE-2020-1179

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.

26525 - (MSPT-May2020) Microsoft Windows GDI Information Disclosure (CVE-2020-0963)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Medium

CVE: CVE-2020-0963

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.

26526 - (MSPT-May2020) Microsoft Windows GDI Information Disclosure (CVE-2020-1145)

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

Risk Level: Medium

CVE: CVE-2020-1145

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 attacker to have valid credentials to the vulnerable system.

26529 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1188)

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

Risk Level: Medium

CVE: CVE-2020-1188

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 State Repository Service 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.

26530 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1189)

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

Risk Level: Medium

CVE: CVE-2020-1189

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 State Repository Service 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.

26531 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1190)

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

Risk Level: Medium

CVE: CVE-2020-1190

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 State Repository Service 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.

26532 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1191)

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

Risk Level: Medium

CVE: CVE-2020-1191

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 State Repository Service 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.

26533 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1184)

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

Risk Level: Medium

CVE: CVE-2020-1184

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 State Repository Service 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.

26534 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1185)

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

Risk Level: Medium

CVE: CVE-2020-1185

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 State Repository Service 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.

26535 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1186)

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

Risk Level: Medium

CVE: CVE-2020-1186

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 State Repository Service 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.

26536 - (MSPT-May2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1187)

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

Risk Level: Medium

CVE: CVE-2020-1187

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 State Repository Service 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.

26537 - (MSPT-May2020) Microsoft Dynamics 365 Improperly Sanitize a Specially Crafted Web Request Spoofing (CVE-2020-1063)

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

Risk Level: Medium

CVE: CVE-2020-1063

Description

A vulnerability in some versions of Microsoft Dynamics 365 could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Dynamics 365 could lead to spoofing.

The flaw lies in improperly sanitize a specially crafted web request. Successful exploitation by a remote attacker could result in spoofing.

26538 - (MSPT-May2020) Microsoft ASP.NET Core Denial of Service (CVE-2020-1161)

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

Risk Level: Medium

CVE: CVE-2020-1161

Description

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

Observation

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

The flaw lies in improperly handles web requests. Successful exploitation by a remote attacker could result in a denial of service

condition.

26539 - (MSPT-May2020) Microsoft .NET Core Denial of Service (CVE-2020-1108)

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

Risk Level: Medium

CVE: CVE-2020-1108

Description

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

Observation

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

The flaw lies in improperly handles web requests. Successful exploitation by a remote attacker could result in a denial of service condition.

131590 - Debian Linux 10.0 DSA-4680-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10072, CVE-2019-12418, CVE-2019-17563, CVE-2019-17569, CVE-2020-1935, CVE-2020-1938

Description

The scan detected that the host is missing the following update:
DSA-4680-1

Observation

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

http://www.debian.org/security/2020/dsa-4680

Debian 10.0
all
tomcat9_9.0.31-1~deb10u1

164217 - Oracle Enterprise Linux ELSA-2020-1998 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2020-11501

Description

The scan detected that the host is missing the following update:
ELSA-2020-1998

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009897.html

OEL8
x86_64
gnutls-3.6.8-10.el8_2
gnutls-c++-3.6.8-10.el8_2
gnutls-devel-3.6.8-10.el8_2
gnutls-dane-3.6.8-10.el8_2
gnutls-utils-3.6.8-10.el8_2

164220 - Oracle Enterprise Linux ELSA-2020-5670 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5244, CVE-2017-7346, CVE-2019-0139, CVE-2019-0140, CVE-2019-0144, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, CVE-2019-19056, CVE-2019-19523, CVE-2019-19527, CVE-2019-19532, CVE-2019-9503, CVE-2020-11494, CVE-2020-8647, CVE-2020-8648, CVE-2020-8649, CVE-2020-9383

Description

The scan detected that the host is missing the following update:
ELSA-2020-5670

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009888.html
http://oss.oracle.com/pipermail/el-errata/2020-May/009889.html

OEL7
x86_64
kernel-uek-debug-4.1.12-124.39.1.el7uek
kernel-uek-firmware-4.1.12-124.39.1.el7uek
kernel-uek-debug-devel-4.1.12-124.39.1.el7uek
kernel-uek-doc-4.1.12-124.39.1.el7uek
kernel-uek-devel-4.1.12-124.39.1.el7uek
kernel-uek-4.1.12-124.39.1.el7uek

OEL6
x86_64
kernel-uek-devel-4.1.12-124.39.1.el6uek
kernel-uek-doc-4.1.12-124.39.1.el6uek
kernel-uek-debug-devel-4.1.12-124.39.1.el6uek
kernel-uek-debug-4.1.12-124.39.1.el6uek
kernel-uek-firmware-4.1.12-124.39.1.el6uek
kernel-uek-4.1.12-124.39.1.el6uek

171218 - Amazon Linux AMI ALAS-2020-1367 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2020-7064, CVE-2020-7066, CVE-2020-7067

Description

The scan detected that the host is missing the following update:
ALAS-2020-1367

Observation

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

https://alas.aws.amazon.com/ALAS-2020-1367.html

Amazon Linux AMI
x86_64
php72-imap-7.2.30-1.22.amzn1
php72-odbc-7.2.30-1.22.amzn1
php72-fpm-7.2.30-1.22.amzn1
php72-xml-7.2.30-1.22.amzn1
php72-7.2.30-1.22.amzn1
php72-tidy-7.2.30-1.22.amzn1
php72-xmlrpc-7.2.30-1.22.amzn1
php72-mbstring-7.2.30-1.22.amzn1
php72-dbg-7.2.30-1.22.amzn1
php72-recode-7.2.30-1.22.amzn1
php72-gmp-7.2.30-1.22.amzn1
php72-bcmath-7.2.30-1.22.amzn1
php72-enchant-7.2.30-1.22.amzn1
php72-gd-7.2.30-1.22.amzn1
php72-opcache-7.2.30-1.22.amzn1
php72-pgsql-7.2.30-1.22.amzn1
php72-process-7.2.30-1.22.amzn1
php72-embedded-7.2.30-1.22.amzn1
php72-pdo-7.2.30-1.22.amzn1
php72-intl-7.2.30-1.22.amzn1
php72-mysqlnd-7.2.30-1.22.amzn1
php72-ldap-7.2.30-1.22.amzn1
php72-common-7.2.30-1.22.amzn1
php72-dba-7.2.30-1.22.amzn1
php72-debuginfo-7.2.30-1.22.amzn1
php72-json-7.2.30-1.22.amzn1
php72-pspell-7.2.30-1.22.amzn1
php72-cli-7.2.30-1.22.amzn1
php72-soap-7.2.30-1.22.amzn1
php72-pdo-dblib-7.2.30-1.22.amzn1
php72-devel-7.2.30-1.22.amzn1
php72-snmp-7.2.30-1.22.amzn1

i686
php72-imap-7.2.30-1.22.amzn1
php72-odbc-7.2.30-1.22.amzn1
php72-fpm-7.2.30-1.22.amzn1
php72-xml-7.2.30-1.22.amzn1
php72-7.2.30-1.22.amzn1
php72-tidy-7.2.30-1.22.amzn1
php72-xmlrpc-7.2.30-1.22.amzn1
php72-mbstring-7.2.30-1.22.amzn1
php72-dbg-7.2.30-1.22.amzn1
php72-recode-7.2.30-1.22.amzn1
php72-gmp-7.2.30-1.22.amzn1
php72-bcmath-7.2.30-1.22.amzn1
php72-gd-7.2.30-1.22.amzn1
php72-opcache-7.2.30-1.22.amzn1
php72-pgsql-7.2.30-1.22.amzn1
php72-process-7.2.30-1.22.amzn1
php72-embedded-7.2.30-1.22.amzn1
php72-pdo-7.2.30-1.22.amzn1

php72-intl-7.2.30-1.22.amzn1
php72-mysqlnd-7.2.30-1.22.amzn1
php72-ldap-7.2.30-1.22.amzn1
php72-common-7.2.30-1.22.amzn1
php72-dba-7.2.30-1.22.amzn1
php72-debuginfo-7.2.30-1.22.amzn1
php72-json-7.2.30-1.22.amzn1
php72-pspell-7.2.30-1.22.amzn1
php72-cli-7.2.30-1.22.amzn1
php72-enchant-7.2.30-1.22.amzn1
php72-soap-7.2.30-1.22.amzn1
php72-pdo-dblib-7.2.30-1.22.amzn1
php72-devel-7.2.30-1.22.amzn1
php72-snmp-7.2.30-1.22.amzn1

171220 - Amazon Linux AMI ALAS-2020-1368 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2020-7064, CVE-2020-7065, CVE-2020-7066, CVE-2020-7067

Description

The scan detected that the host is missing the following update:
ALAS-2020-1368

Observation

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

https://alas.aws.amazon.com/ALAS-2020-1368.html

Amazon Linux AMI
x86_64
php73-debuginfo-7.3.17-1.25.amzn1
php73-xml-7.3.17-1.25.amzn1
php73-gmp-7.3.17-1.25.amzn1
php73-common-7.3.17-1.25.amzn1
php73-pdo-7.3.17-1.25.amzn1
php73-json-7.3.17-1.25.amzn1
php73-odbc-7.3.17-1.25.amzn1
php73-mysqlnd-7.3.17-1.25.amzn1
php73-fpm-7.3.17-1.25.amzn1
php73-soap-7.3.17-1.25.amzn1
php73-pspell-7.3.17-1.25.amzn1
php73-dba-7.3.17-1.25.amzn1
php73-devel-7.3.17-1.25.amzn1
php73-enchant-7.3.17-1.25.amzn1
php73-dbg-7.3.17-1.25.amzn1
php73-xmlrpc-7.3.17-1.25.amzn1
php73-cli-7.3.17-1.25.amzn1
php73-7.3.17-1.25.amzn1
php73-pgsql-7.3.17-1.25.amzn1
php73-ldap-7.3.17-1.25.amzn1
php73-bcmath-7.3.17-1.25.amzn1
php73-embedded-7.3.17-1.25.amzn1
php73-pdo-dblib-7.3.17-1.25.amzn1
php73-opcache-7.3.17-1.25.amzn1
php73-snmp-7.3.17-1.25.amzn1

php73-gd-7.3.17-1.25.amzn1
php73-recode-7.3.17-1.25.amzn1
php73-mbstring-7.3.17-1.25.amzn1
php73-tidy-7.3.17-1.25.amzn1
php73-intl-7.3.17-1.25.amzn1
php73-process-7.3.17-1.25.amzn1
php73-imap-7.3.17-1.25.amzn1

i686
php73-debuginfo-7.3.17-1.25.amzn1
php73-xml-7.3.17-1.25.amzn1
php73-gmp-7.3.17-1.25.amzn1
php73-common-7.3.17-1.25.amzn1
php73-pdo-7.3.17-1.25.amzn1
php73-json-7.3.17-1.25.amzn1
php73-mysqlnd-7.3.17-1.25.amzn1
php73-fpm-7.3.17-1.25.amzn1
php73-soap-7.3.17-1.25.amzn1
php73-pspell-7.3.17-1.25.amzn1
php73-devel-7.3.17-1.25.amzn1
php73-enchant-7.3.17-1.25.amzn1
php73-dbg-7.3.17-1.25.amzn1
php73-xmlrpc-7.3.17-1.25.amzn1
php73-cli-7.3.17-1.25.amzn1
php73-opcache-7.3.17-1.25.amzn1
php73-7.3.17-1.25.amzn1
php73-pgsql-7.3.17-1.25.amzn1
php73-ldap-7.3.17-1.25.amzn1
php73-bcmath-7.3.17-1.25.amzn1
php73-embedded-7.3.17-1.25.amzn1
php73-pdo-dblib-7.3.17-1.25.amzn1
php73-odbc-7.3.17-1.25.amzn1
php73-snmp-7.3.17-1.25.amzn1
php73-intl-7.3.17-1.25.amzn1
php73-gd-7.3.17-1.25.amzn1
php73-recode-7.3.17-1.25.amzn1
php73-mbstring-7.3.17-1.25.amzn1
php73-tidy-7.3.17-1.25.amzn1
php73-dba-7.3.17-1.25.amzn1
php73-process-7.3.17-1.25.amzn1
php73-imap-7.3.17-1.25.amzn1

178857 - Gentoo Linux GLSA-202005-04 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-202005-04

Observation

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

https://security.gentoo.org/glsa/202005-04

Affected packages:
www-client/firefox < 68.8.0
www-client/firefox-bin < 68.8.0

178858 - Gentoo Linux GLSA-202005-10 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-202005-10

Observation

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

https://security.gentoo.org/glsa/202005-10

Affected packages:
net-libs/libmicrodns < 0.1.2

178859 - Gentoo Linux GLSA-202005-11 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-202005-11

Observation

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

https://security.gentoo.org/glsa/202005-11

Affected packages:
media-video/vlc < 3.0.10

178860 - Gentoo Linux GLSA-202005-07 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-202005-07

Observation

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

https://security.gentoo.org/glsa/202005-07

Affected packages:
net-misc/freerdp < 2.1.0

178862 - Gentoo Linux GLSA-202005-02 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-202005-02

Observation

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

https://security.gentoo.org/glsa/202005-02

Affected packages:
app-emulation/qemu < 4.2.0-r5

178863 - Gentoo Linux GLSA-202005-12 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-202005-12

Observation

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

https://security.gentoo.org/glsa/202005-12

Affected packages:
net-misc/openslp <= 2.0.0-r5

178865 - Gentoo Linux GLSA-202005-03 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-202005-03

Observation

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

https://security.gentoo.org/glsa/202005-03

Affected packages:
mail-client/thunderbird < 68.8.0
mail-client/thunderbird-bin < 68.8.0

178866 - Gentoo Linux GLSA-202005-13 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-202005-13

Observation

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

https://security.gentoo.org/glsa/202005-13

Affected packages:
www-client/chromium < 81.0.4044.138
www-client/google-chrome < 81.0.4044.138

178867 - Gentoo Linux GLSA-202005-06 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-202005-06

Observation

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

https://security.gentoo.org/glsa/202005-06

Affected packages:
media-plugins/live < 2020.03.06

178868 - Gentoo Linux GLSA-202005-08 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-202005-08

Observation

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

https://security.gentoo.org/glsa/202005-08

Affected packages:
app-emulation/xen < 4.12.2-r2
app-emulation/xen-tools < 4.12.2-r1

196724 - Red Hat Enterprise Linux RHSA-2020-2068 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18074, CVE-2018-20060, CVE-2019-11236, CVE-2019-11324

Description

The scan detected that the host is missing the following update:
RHSA-2020-2068

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00043.html

RHEL7D
noarch
python3-pip-9.0.3-7.el7_8

RHEL7S
noarch
python3-pip-9.0.3-7.el7_8

RHEL7WS
noarch
python3-pip-9.0.3-7.el7_8

196726 - Red Hat Enterprise Linux RHSA-2020-2081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18074, CVE-2018-20060, CVE-2019-11236

Description

The scan detected that the host is missing the following update:
RHSA-2020-2081

Observation

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

http://www.redhat.com/archives/rhsa-announce/2020-May/msg00045.html

RHEL7D
noarch
python-virtualenv-15.1.0-4.el7_8

RHEL7S
noarch
python-virtualenv-15.1.0-4.el7_8

RHEL7WS
noarch
python-virtualenv-15.1.0-4.el7_8

26476 - (MSPT-May2020) Microsoft Edge Chakra Remote Code Execution (CVE-2020-1037)

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

Risk Level: Medium

CVE: CVE-2020-1037

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.

26490 - (MSPT-May2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1065)

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

Risk Level: Medium

CVE: CVE-2020-1065

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 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.

26495 - (MSPT-May2020) Microsoft Edge PDF Reader Remote Code Execution (CVE-2020-1096)

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

Risk Level: Medium

CVE: CVE-2020-1096

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 PDF Reader 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.

26499 - (MSPT-May2020) Microsoft Windows Connected User Experiences and Telemetry Service Denial of Service (CVE-2020-1084)

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

Risk Level: Medium

CVE: CVE-2020-1084

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 in the Connected User Experiences and Telemetry Service component. Successful exploitation by an attacker could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.

164224 - Oracle Enterprise Linux ELSA-2020-5671 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7261, CVE-2019-19527, CVE-2019-19532, CVE-2019-9503

Description

The scan detected that the host is missing the following update:
ELSA-2020-5671

Observation

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

http://oss.oracle.com/pipermail/el-errata/2020-May/009900.html
http://oss.oracle.com/pipermail/el-errata/2020-May/009899.html

OEL7
x86_64
kernel-uek-3.8.13-118.45.1.el7uek
kernel-uek-debug-devel-3.8.13-118.45.1.el7uek
kernel-uek-doc-3.8.13-118.45.1.el7uek
dtrace-modules-3.8.13-118.45.1.el7uek-0.4.5-3.el7
kernel-uek-firmware-3.8.13-118.45.1.el7uek
kernel-uek-debug-3.8.13-118.45.1.el7uek

kernel-uek-devel-3.8.13-118.45.1.el7uek

OEL6
x86_64
kernel-uek-debug-3.8.13-118.45.1.el6uek
kernel-uek-doc-3.8.13-118.45.1.el6uek
kernel-uek-devel-3.8.13-118.45.1.el6uek
kernel-uek-3.8.13-118.45.1.el6uek
dtrace-modules-3.8.13-118.45.1.el6uek-0.4.5-3.el6
kernel-uek-debug-devel-3.8.13-118.45.1.el6uek
kernel-uek-firmware-3.8.13-118.45.1.el6uek

183272 - FreeBSD glpi Stored XSS (d222241d-91cc-11ea-82b8-4c72b94353b5)

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

Risk Level: Medium

CVE: CVE-2019-13239

Description

The scan detected that the host is missing the following update:
glpi -- stored XSS (d222241d-91cc-11ea-82b8-4c72b94353b5)

Observation

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

http://www.vuxml.org/freebsd/d222241d-91cc-11ea-82b8-4c72b94353b5.html

Affected packages:
glpi < 9.4.3

131578 - Debian Linux 10.0, 9.0 DSA-4678-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
DSA-4678-1

Observation

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

http://www.debian.org/security/2020/dsa-4678

Debian 9.0
all
firefox-esr_68.8.0esr-1~deb9u1

Debian 10.0
all
firefox-esr_68.8.0esr-1~deb10u1

131579 - Debian Linux 10.0 DSA-4681-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-3885, CVE-2020-3894, CVE-2020-3895, CVE-2020-3897, CVE-2020-3899, CVE-2020-3900, CVE-2020-3901, CVE-2020-3902

Description

The scan detected that the host is missing the following update:
DSA-4681-1

Observation

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

http://www.debian.org/security/2020/dsa-4681

Debian 10.0
all
libwebkit2gtk-4.0-37_2.28.2-2~deb10u1
gir1.2-webkit2-4.0_2.28.2-2~deb10u1
libwebkit2gtk-4.0-37-gtk2_2.28.2-2~deb10u1
libwebkit2gtk-4.0-doc_2.28.2-2~deb10u1
libjavascriptcoregtk-4.0-bin_2.28.2-2~deb10u1
gir1.2-javascriptcoregtk-4.0_2.28.2-2~deb10u1
libwebkit2gtk-4.0-dev_2.28.2-2~deb10u1
libjavascriptcoregtk-4.0-dev_2.28.2-2~deb10u1
libjavascriptcoregtk-4.0-18_2.28.2-2~deb10u1
webkit2gtk-driver_2.28.2-2~deb10u1

131580 - Debian Linux 10.0 DSA-4679-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-4679-1

Observation

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

http://www.debian.org/security/2020/dsa-4679

Debian 10.0
all
keystone_2:14.2.0-0+deb10u1

131581 - Debian Linux 10.0 DSA-4682-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-12519, CVE-2019-12520, CVE-2019-12521, CVE-2019-12523, CVE-2019-12524, CVE-2019-12526, CVE-2019-

12528, CVE-2019-18676, CVE-2019-18677, CVE-2019-18678, CVE-2019-18679, CVE-2020-11945, CVE-2020-8449, CVE-2020-8450

Description

The scan detected that the host is missing the following update:
DSA-4682-1

Observation

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

http://www.debian.org/security/2020/dsa-4682

Debian 10.0
all
squid_4.6-1+deb10u2

131582 - Debian Linux 10.0, 9.0 DSA-4683-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-12387, CVE-2020-12392, CVE-2020-12395, CVE-2020-12397, CVE-2020-6831

Description

The scan detected that the host is missing the following update:
DSA-4683-1

Observation

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

http://www.debian.org/security/2020/dsa-4683

Debian 9.0
all
thunderbird_1:68.8.0-1~deb9u1

Debian 10.0
all
thunderbird_1:68.8.0-1~deb10u1

131583 - Debian Linux 10.0, 9.0 DSA-4675-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-12921, CVE-2020-10938

Description

The scan detected that the host is missing the following update:
DSA-4675-1

Observation

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

http://www.debian.org/security/2020/dsa-4675

Debian 9.0
all
graphicsmagick_1.3.30+hg15796-1~deb9u4

Debian 10.0
all
graphicsmagick_1.4+really1.3.35-1~deb10u1

131584 - Debian Linux 10.0, 9.0 DSA-4676-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-17361, CVE-2020-11651, CVE-2020-11652

Description

The scan detected that the host is missing the following update:
DSA-4676-1

Observation

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

http://www.debian.org/security/2020/dsa-4676

Debian 9.0
all
salt-proxy_2016.11.2+ds-1+deb9u3
salt-minion_2016.11.2+ds-1+deb9u3
salt-doc_2016.11.2+ds-1+deb9u3
salt-cloud_2016.11.2+ds-1+deb9u3
salt-master_2016.11.2+ds-1+deb9u3
salt-common_2016.11.2+ds-1+deb9u3
salt-api_2016.11.2+ds-1+deb9u3
salt-ssh_2016.11.2+ds-1+deb9u3
salt-syndic_2016.11.2+ds-1+deb9u3

Debian 10.0
all
salt-master_2018.3.4+dfsg1-6+deb10u1
salt-minion_2018.3.4+dfsg1-6+deb10u1
salt-syndic_2018.3.4+dfsg1-6+deb10u1
salt-common_2018.3.4+dfsg1-6+deb10u1
salt-ssh_2018.3.4+dfsg1-6+deb10u1
salt-cloud_2018.3.4+dfsg1-6+deb10u1
salt-doc_2018.3.4+dfsg1-6+deb10u1
salt-api_2018.3.4+dfsg1-6+deb10u1
salt-proxy_2018.3.4+dfsg1-6+deb10u1

131586 - Debian Linux 10.0 DSA-4684-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-1763

Description

The scan detected that the host is missing the following update:
DSA-4684-1

Observation

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

http://www.debian.org/security/2020/dsa-4684

Debian 10.0
all
libreswan_3.27-6+deb10u1

131587 - Debian Linux 10.0, 9.0 DSA-4685-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-3810

Description

The scan detected that the host is missing the following update:
DSA-4685-1

Observation

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

http://www.debian.org/security/2020/dsa-4685

Debian 9.0
all
apt_1.4.10

Debian 10.0
all
apt_1.8.2.1

131588 - Debian Linux 10.0, 9.0 DSA-4686-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-17571

Description

The scan detected that the host is missing the following update:
DSA-4686-1

Observation

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

http://www.debian.org/security/2020/dsa-4686

Debian 9.0
all

liblog4j1.2-java_1.2.17-7+deb9u1
liblog4j1.2-java-doc_1.2.17-7+deb9u1

Debian 10.0
all
liblog4j1.2-java-doc_1.2.17-8+deb10u1
liblog4j1.2-java_1.2.17-8+deb10u1

131589 - Debian Linux 10.0, 9.0 DSA-4687-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-12783

Description

The scan detected that the host is missing the following update:
DSA-4687-1

Observation

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

http://www.debian.org/security/2020/dsa-4687

Debian 9.0
all
exim4_4.89-2+deb9u7

Debian 10.0
all
exim4_4.92-8+deb10u4

178864 - Gentoo Linux GLSA-202005-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-202005-01

Observation

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

https://security.gentoo.org/glsa/202005-01

Affected packages:
app-arch/lrzip < 0.631_p20190619

183271 - FreeBSD FreeBSD Insufficient Packet Length Validation In Libalias (30ce591c-947b-11ea-92ab-00163e433440)

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

Risk Level: Low

CVE: CVE-2020-7454

Description

The scan detected that the host is missing the following update:
FreeBSD -- Insufficient packet length validation in libalias (30ce591c-947b-11ea-92ab-00163e433440)

Observation

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

http://www.vuxml.org/freebsd/30ce591c-947b-11ea-92ab-00163e433440.html

Affected packages:
12.1 <= FreeBSD-kernel < 12.1_5
11.4 <= FreeBSD-kernel < 11.4_1
11.3 <= FreeBSD-kernel < 11.3_9

183273 - FreeBSD FreeBSD Use After Free In Cryptodev Module (9f15c2da-947e-11ea-92ab-00163e433440)

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

Risk Level: Low

CVE: CVE-2019-15879

Description

The scan detected that the host is missing the following update:
FreeBSD -- Use after free in cryptodev module (9f15c2da-947e-11ea-92ab-00163e433440)

Observation

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

http://www.vuxml.org/freebsd/9f15c2da-947e-11ea-92ab-00163e433440.html

Affected packages:
12.1 <= FreeBSD-kernel < 12.1_5
11.3 <= FreeBSD-kernel < 11.3_9

183274 - FreeBSD typo3 Multiple Vulnerabilities (59fabdf2-9549-11ea-9448-08002728f74c)

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

Risk Level: Low

CVE: CVE-2020-11063, CVE-2020-11064, CVE-2020-11065, CVE-2020-11066, CVE-2020-11067, CVE-2020-11069

Description

The scan detected that the host is missing the following update:
typo3 -- multiple vulnerabilities (59fabdf2-9549-11ea-9448-08002728f74c)

Observation

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

http://www.vuxml.org/freebsd/59fabdf2-9549-11ea-9448-08002728f74c.html

Affected packages:
typo3-9-php72 < 9.5.17

typo3-9-php73 < 9.5.17
typo3-9-php74 < 9.5.17
typo3-10-php72 < 10.4.2
typo3-10-php73 < 10.4.2
typo3-10-php74 < 10.4.2

183275 - FreeBSD qutebrowser Reloading Page With Certificate Errors Shows A Green URL (452d16bb-920d-11ea-9d20-18a6f7016652)

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

Risk Level: Low

CVE: CVE-2020-11054

Description

The scan detected that the host is missing the following update:
qutebrowser -- Reloading page with certificate errors shows a green URL (452d16bb-920d-11ea-9d20-18a6f7016652)

Observation

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

http://www.vuxml.org/freebsd/452d16bb-920d-11ea-9d20-18a6f7016652.html

Affected packages:
qutebrowser < 1.11.1

183276 - FreeBSD FreeBSD Memory Disclosure Vulnerability In Libalias (78992249-947c-11ea-92ab-00163e433440)

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

Risk Level: Low

CVE: CVE-2020-7455

Description

The scan detected that the host is missing the following update:
FreeBSD -- Memory disclosure vulnerability in libalias (78992249-947c-11ea-92ab-00163e433440)

Observation

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

http://www.vuxml.org/freebsd/78992249-947c-11ea-92ab-00163e433440.html

Affected packages:
12.1 <= FreeBSD-kernel < 12.1_5
11.4 <= FreeBSD-kernel < 11.4_1
11.3 <= FreeBSD-kernel < 11.3_9

183277 - FreeBSD salt Multiple Vulnerabilities In Salt-master Process (6bf55af9-973b-11ea-9f2c-38d547003487)

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

Risk Level: Low

CVE: CVE-2020-11651, CVE-2020-11652

Description

The scan detected that the host is missing the following update:
salt -- multiple vulnerabilities in salt-master process (6bf55af9-973b-11ea-9f2c-38d547003487)

Observation

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

http://www.vuxml.org/freebsd/6bf55af9-973b-11ea-9f2c-38d547003487.html

Affected packages:
py27-salt < 2019.2.4
py32-salt < 2019.2.4
py33-salt < 2019.2.4
py34-salt < 2019.2.4
py35-salt < 2019.2.4
py36-salt < 2019.2.4
py37-salt < 2019.2.4
py38-salt < 2019.2.4
3000 <= py27-salt < 3000.2
3000 <= py32-salt < 3000.2
3000 <= py33-salt < 3000.2
3000 <= py34-salt < 3000.2
3000 <= py35-salt < 3000.2
3000 <= py36-salt < 3000.2
3000 <= py37-salt < 3000.2
3000 <= py38-salt < 3000.2

183278 - FreeBSD FreeBSD Improper Checking In SCTP-AUTH Shared Key Update (253486f5-947d-11ea-92ab-00163e433440)

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

Risk Level: Low

CVE: CVE-2019-15878

Description

The scan detected that the host is missing the following update:
FreeBSD -- Improper checking in SCTP-AUTH shared key update (253486f5-947d-11ea-92ab-00163e433440)

Observation

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

http://www.vuxml.org/freebsd/253486f5-947d-11ea-92ab-00163e433440.html

Affected packages:
11.3 <= FreeBSD-kernel < 11.3_9

183279 - FreeBSD clamav Multiple Vulnerabilities (91ce95d5-cd15-4105-b942-af5ccc7144c1)

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

Risk Level: Low

CVE: CVE-2020-3327, CVE-2020-3341

Description

The scan detected that the host is missing the following update:
clamav -- multiple vulnerabilities (91ce95d5-cd15-4105-b942-af5ccc7144c1)

Observation

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

http://www.vuxml.org/freebsd/91ce95d5-cd15-4105-b942-af5ccc7144c1.html

Affected packages:
clamav < 0.102.3,1

183280 - FreeBSD zeek Various Vulnerabilities (1a6b7641-aed2-4ba1-96f4-c282d5b09c37)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
zeek -- Various vulnerabilities (1a6b7641-aed2-4ba1-96f4-c282d5b09c37)

Observation

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

http://www.vuxml.org/freebsd/1a6b7641-aed2-4ba1-96f4-c282d5b09c37.html

Affected packages:
zeek < 3.0.6

183281 - FreeBSD FreeBSD Insufficient Cryptodev MAC Key Length Check (0bfcae0b-947f-11ea-92ab-00163e433440)

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

Risk Level: Low

CVE: CVE-2019-15879

Description

The scan detected that the host is missing the following update:
FreeBSD -- Insufficient cryptodev MAC key length check (0bfcae0b-947f-11ea-92ab-00163e433440)

Observation

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

http://www.vuxml.org/freebsd/0bfcae0b-947f-11ea-92ab-00163e433440.html

Affected packages:
12.1 <= FreeBSD-kernel < 12.1_5

183282 - FreeBSD json-c Integer Overflow And Out-of-bounds Write Via A Large JSON File (abc3ef37-95d4-11ea-9004-25fadb81abf4)

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

Risk Level: Low

CVE: CVE-2020-12762

Description

The scan detected that the host is missing the following update:
json-c -- integer overflow and out-of-bounds write via a large JSON file (abc3ef37-95d4-11ea-9004-25fadb81abf4)

Observation

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

http://www.vuxml.org/freebsd/abc3ef37-95d4-11ea-9004-25fadb81abf4.html

Affected packages:
json-c < 0.14

183283 - FreeBSD Python CRLF Injection Via The Host Part Of The Url Passed To Urlopen () (ca595a25-91d8-11ea-b470-080027846a02)

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

Risk Level: Low

CVE: CVE-2019-18348

Description

The scan detected that the host is missing the following update:
Python -- CRLF injection via the host part of the url passed to urlopen() (ca595a25-91d8-11ea-b470-080027846a02)

Observation

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

http://www.vuxml.org/freebsd/ca595a25-91d8-11ea-b470-080027846a02.html

Affected packages:
python27 < 2.7.18

183284 - FreeBSD Rails Remote Code Execution Vulnerability (ce6db19b-976e-11ea-93c4-08002728f74c)

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

Risk Level: Low

CVE: CVE-2020-8163

Description

The scan detected that the host is missing the following update:
Rails -- remote code execution vulnerability (ce6db19b-976e-11ea-93c4-08002728f74c)

Observation

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

http://www.vuxml.org/freebsd/ce6db19b-976e-11ea-93c4-08002728f74c.html

Affected packages:
rubygem-actionview4 < 4.2.11.2

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.

183254 - FreeBSD MySQL Server Multiple Vulerabilities (21d59ea3-8559-11ea-a5e2-d4c9ef517024)

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

Risk Level: High

CVE: CVE-2019-1547, CVE-2019-15601, CVE-2019-5482, CVE-2020-2759, CVE-2020-2760, CVE-2020-2761, CVE-2020-2762, CVE-2020-2763, CVE-2020-2765, CVE-2020-2768, CVE-2020-2770, CVE-2020-2774, CVE-2020-2779, CVE-2020-2780, CVE-2020-2790, CVE-2020-2804, CVE-2020-2806, CVE-2020-2812, CVE-2020-2814, CVE-2020-2853, CVE-2020-2892, CVE-2020-2893, CVE-2020-2895, CVE-2020-2896, CVE-2020-2897, CVE-2020-2898, CVE-2020-2901, CVE-2020-2903, CVE-2020-2904, CVE-2020-2921, CVE-2020-2923, CVE-2020-2924, CVE-2020-2925, CVE-2020-2926, CVE-2020-2928, CVE-2020-2930

Update Details

FASLScript is updated

183266 - FreeBSD mailman Content Injection Vulnerability Via Options Login Page (88760f4d-8ef7-11ea-a66d-4b2ef158be83)

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

Risk Level: Medium

CVE: CVE-2018-13796

Update Details

FASLScript is updated

131571 - Debian Linux 10.0 DSA-4667-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2020-10942, CVE-2020-11565, CVE-2020-11884, CVE-2020-2732, CVE-2020-8428

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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