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

26127 - (APSB20-06) Vulnerability In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-3757

Description
A vulnerability in some versions of Adobe Flash Player could lead to remote code execution.

Observation
A vulnerability in some versions of Adobe Flash Player could lead to remote code execution.

The flaw lies in an unknown component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

196600 - Red Hat Enterprise Linux RHSA-2020-0513 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-3757

Description
The scan detected that the host is missing the following update:
RHSA-2020-0513

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

RHEL6D
x86_64
flash-plugin-32.0.0.330-1.el6_10

i386
flash-plugin-32.0.0.330-1.el6_10

RHEL6S
x86_64
flash-plugin-32.0.0.330-1.el6_10

i386

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: High  
CVE: CVE-2020-0655  

**Description**  
A vulnerability in some versions of Microsoft Remote Desktop Services could lead to remote code execution.

**Observation**  
A vulnerability in some versions of Microsoft Remote Desktop Services could lead to remote code execution.  
The flaw lies in the Clipboard Redirection component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

**26115 - (MSPT-Feb2020) Microsoft SharePoint Server XSS Vulnerability (CVE-2020-0693)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: High  
CVE: CVE-2020-0693  

**Description**  
A vulnerability in some versions of Microsoft SharePoint Server could lead to a cross-site scripting attack.

**Observation**  
A vulnerability in some versions of Microsoft SharePoint Server could lead to a cross-site scripting attack.  
The flaw lies in improperly sanitize a specially crafted web request. Successful exploitation by a remote attacker could result in a cross-site scripting attack.

**26116 - (MSPT-Feb2020) Microsoft SharePoint Server XSS Vulnerability (CVE-2020-0694)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: High  
CVE: CVE-2020-0694  

**Description**  
A vulnerability in some versions of Microsoft SharePoint Server could lead to a cross-site scripting attack.

**Observation**  
A vulnerability in some versions of Microsoft SharePoint Server could lead to a cross-site scripting attack.
The flaw lies in improperly sanitize a specially crafted web request. Successful exploitation by a remote attacker could result in a cross-site scripting attack.

**26122 - (MSPT-Feb2020) Microsoft Windows Graphics Component Privilege Escalation (CVE-2020-0792)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0792

**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.

**26028 - (MSPT-Feb2020) Microsoft Win32k Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0719)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0719

**Description**
A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Win32k 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.

**26060 - (MSPT-Feb2020) Microsoft Win32k Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0724)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0724

**Description**
A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Win32k 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.

**26062 - (MSPT-Feb2020) Microsoft Win32k Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0723)**
A vulnerability in some versions of Microsoft Win32k 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.
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.

**26066 - (MSPT-Feb2020) Microsoft Win32k Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0725)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0725

Description
A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Win32k 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.

**26068 - (MSPT-Feb2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-0671)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0671

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.

**26069 - (MSPT-Feb2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-0672)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0672

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.

26078 - (MSPT-Feb2020) Microsoft Windows ChakraCore Remote Code Execution (CVE-2020-0767)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0767

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 ChakraCore component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

26079 - (MSPT-Feb2020) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2020-0674)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0674

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

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

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

26080 - (MSPT-Feb2020) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2020-0673)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0673

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

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

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

The flaw lies in the Remote Desktop Client component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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

The flaw lies in the Remote Desktop Client component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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

The flaw lies in the RDP component. Successful exploitation by a remote attacker could result in a denial of service condition.

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

The flaw lies in the Data Sharing Service component. Successful exploitation by a remote attacker could result in privilege escalation.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Data Sharing 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.

**26107 - (MSPT-Feb2020) Microsoft Tapisrv.dll Privilege Escalation (CVE-2020-0737)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0737

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

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

**26109 - (MSPT-Feb2020) Microsoft Windows Hyper-V Denial of Service (CVE-2020-0751)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0751

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

The flaw lies in the Hyper-V 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.

**26113 - (MSPT-Feb2020) Microsoft Windows Hyper-V Denial of Service (CVE-2020-0661)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0661

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

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

**26114 - (MSPT-Feb2020) Microsoft Windows Improperly Handles Objects In Memory Remote Code Execution (CVE-2020-0662)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0662

**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 attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0759

**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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-0696

**Description**
A vulnerability in some versions of Microsoft Outlook could lead to remote code execution.

**Observation**
A vulnerability in some versions of Microsoft Outlook could lead to remote code execution.

The flaw lies in improperly handles parsing of URI formats. Successful exploitation by a remote attacker could result in the
A vulnerability in some versions of Microsoft Exchange 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.

A vulnerability in some versions of Microsoft SQL Server could lead to remote code execution. The flaw lies in the Reporting Services 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.

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat. The flaws lie in undetermined components. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.
The update provided by Adobe bulletin APSB20-05 resolves these issues.

### 26125 - (MSPT-Feb2020) Microsoft Windows Remote Desktop Client Remote Code Execution (CVE-2020-0817)

**Category:** Windows Host Assessment -> Patches and Hotfixes  
*(CATEGORY REQUIRES CREDENTIALS)*  
**Risk Level:** High  
**CVE:** CVE-2020-0817

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

**Observation**  
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.  
The flaw lies in the Remote Desktop Client component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### 26126 - (MSPT-Feb2020) Microsoft Sysmain.dll Privilege Escalation (CVE-2020-0818)

**Category:** Windows Host Assessment -> Patches and Hotfixes  
*(CATEGORY REQUIRES CREDENTIALS)*  
**Risk Level:** High  
**CVE:** CVE-2020-0818

**Description**  
A vulnerability in some versions of Microsoft Sysmain.dll could lead to privilege escalation.

**Observation**  
A vulnerability in some versions of Microsoft Sysmain.dll 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.

### 148741 - SuSE SLES 12 SP4, 12 SP5, SLED 12 SP4 SUSE-SU-2020:0360-1 Update Is Not Installed

**Category:** SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes  
**Risk Level:** High  
**CVE:** CVE-2019-5188

**Description**  
The scan detected that the host is missing the following update:  
SUSE-SU-2020:0360-1

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

SuSE SLES 12 SP4  
x86_64  
libcom_err2-debuginfo-1.43.8-3.11.1
Description
The scan detected that the host is missing the following update:
SUSE-SU-2020:0351-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
148743 - SuSE Linux 15.1 openSUSE-SU-2020:0170-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0170-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00019.html

SuSE Linux 15.1
i586
libMagickCore-7_Q16HDRI6-debuginfo-7.0.7.34-lp151.7.15.1
libMagick++-7_Q16HDR14-debuginfo-7.0.7.34-lp151.7.15.1
ImageMagick-debugsource-7.0.7.34-lp151.7.15.1
libMagickWand-7_Q16HDR16-debuginfo-7.0.7.34-lp151.7.15.1
libMagickCore-7_Q16HDR16-7.0.7.34-lp151.7.15.1
libMagickWand-7_Q16HDR16-7.0.7.34-lp151.7.15.1
libMagick++-7_Q16HDR14-7.0.7.34-lp151.7.15.1
ImageMagick-extra-7.0.7.34-lp151.7.15.1
ImageMagick-config-7-SUSE-7.0.7.34-lp151.7.15.1
ImageMagick-devel-7.0.7.34-lp151.7.15.1
perl-PerlMagick-debuginfo-7.0.7.34-lp151.7.15.1
libMagick++-devel-7.0.7.34-lp151.7.15.1
ImageMagick-7.0.7.34-lp151.7.15.1
perl-PerlMagick-7.0.7.34-lp151.7.15.1
ImageMagick-extra-debuginfo-7.0.7.34-lp151.7.15.1
ImageMagick-config-7-upstream-7.0.7.34-lp151.7.15.1
ImageMagick-debuginfo-7.0.7.34-lp151.7.15.1
noarch
ImageMagick-doc-7.0.7.34-lp151.7.15.1

x86_64
libMagick++-devel-32bit-7.0.7.34-lp151.7.15.1
libMagickCore-7_Q16HDR16-debuginfo-7.0.7.34-lp151.7.15.1
libMagickWand-7_Q16HDR16-32bit-7.0.7.34-lp151.7.15.1
libMagickCore-7_Q16HDR16-32bit-7.0.7.34-lp151.7.15.1
libMagick++-7_Q16HDR14-debuginfo-7.0.7.34-lp151.7.15.1
ImageMagick-debugsource-7.0.7.34-lp151.7.15.1
libMagickWand-7_Q16HDR16-debuginfo-7.0.7.34-lp151.7.15.1
libMagickCore-7_Q16HDR16-7.0.7.34-lp151.7.15.1
libMagick++-7_Q16HDR14-7.0.7.34-lp151.7.15.1
ImageMagick-extra-7.0.7.34-lp151.7.15.1
ImageMagick-devel-32bit-7.0.7.34-lp151.7.15.1
ImageMagick-config-7-SUSE-7.0.7.34-lp151.7.15.1
libMagickCore-7_Q16HDR16-32bit-debuginfo-7.0.7.34-lp151.7.15.1
ImageMagick-devel-7.0.7.34-lp151.7.15.1
libMagick++-7_Q16HDR14-32bit-7.0.7.34-lp151.7.15.1
perl-PerlMagick-debuginfo-7.0.7.34-lp151.7.15.1
libMagick++-32bit-7.0.7.34-lp151.7.15.1
**148744 - SuSE Linux 15.1 openSUSE-SU-2020:0209-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2020-0569

**Description**

The scan detected that the host is missing the following update:
openSUSE-SU-2020:0209-1

**Observation**

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

https://lists.opensuse.org/opensuse-updates/2020-02/msg00053.html

SuSE Linux 15.1

i586
libQt5OpenGLExtensions-devel-static-5.9.7-lp151.4.3.1
libQt5DBus5-debuginfo-5.9.7-lp151.4.3.1
libQt5Sql5-debuginfo-5.9.7-lp151.4.3.1
libqt5-qtbase-common-devel-5.9.7-lp151.4.3.1
libQt5Xml5-debuginfo-5.9.7-lp151.4.3.1
libQt5Widgets5-5.9.7-lp151.4.3.1
libQt5Test-devel-5.9.7-lp151.4.3.1
libQt5Xml5-5.9.7-lp151.4.3.1
libQt5Core-devel-5.9.7-lp151.4.3.1
libQt5Core5-5.9.7-lp151.4.3.1
libqt5-qtbase-platformtheme-gtk3-debuginfo-5.9.7-lp151.4.3.1
libQt5PlatformSupport-devel-static-5.9.7-lp151.4.3.1
libQt5Gui-devel-5.9.7-lp151.4.3.1
libQt5Concurrent-devel-5.9.7-lp151.4.3.1
libQt5Sql5- unixODBC-5.9.7-lp151.4.3.1
libQt5Widgets-devel-5.9.7-lp151.4.3.1
libQt5Sql5-postgresql-debuginfo-5.9.7-lp151.4.3.1
libQt5Sql5-postgresql-5.9.7-lp151.4.3.1
libQt5Network-devel-5.9.7-lp151.4.3.1
libQt5PlatformHeaders-devel-5.9.7-lp151.4.3.1
libQt5Concurrent-devel-5.9.7-lp151.4.3.1
libQt5Test5-debuginfo-5.9.7-lp151.4.3.1
libqt5-qtbase- debugsource-5.9.7-lp151.4.3.1
libQt5Gui5-debuginfo-5.9.7-lp151.4.3.1
libQt5Widgets5-debuginfo-5.9.7-lp151.4.3.1
libQt5Bootstrap-devel-static-5.9.7-lp151.4.3.1
libQt5OpenGL-devel-5.9.7-lp151.4.3.1
libqt5-qtbase-examples-debuginfo-5.9.7-lp151.4.3.1
libQt5Test5-5.9.7-lp151.4.3.1
libQt5Core5-debuginfo-5.9.7-lp151.4.3.1
libqt5-qtbase-examples-5.9.7-lp151.4.3.1
libQt5Sql5-mysql-debuginfo-5.9.7-lp151.4.3.1
libQt5Concurrent-devel-5.9.7-lp151.4.3.1
libQt5PrintSupport-devel-5.9.7-lp151.4.3.1
libQt5Sql5-32bit-5.9.7-lp151.4.3.1
libQt5Core-devel-32bit-5.9.7-lp151.4.3.1
libQt5PlatformHeaders-devel-5.9.7-lp151.4.3.1
libQt5Gui5-5.9.7-lp151.4.3.1
libQt5Sql5-unixODBC-5.9.7-lp151.4.3.1
libQt5Concurrent5-debuginfo-5.9.7-lp151.4.3.1
libQt5PrintSupport5-debuginfo-5.9.7-lp151.4.3.1
libQt5Concurrent5-32bit-5.9.7-lp151.4.3.1
libqt5-qtbase-examples-debuginfo-5.9.7-lp151.4.3.1

148745 - SuSE SLED 12 SP4, 12 SP5 SUSE-SU-2020:0324-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-17626

Description
The scan detected that the host is missing the following update:
SUSE-SU-2020:0324-1

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

SuSE SLED 12 SP4
x86_64
python-reportlab-debuginfo-2.7-3.3.1
python-reportlab-2.7-3.3.1
python-reportlab-debugsource-2.7-3.3.1

SuSE SLED 12 SP5
x86_64
python-reportlab-debuginfo-2.7-3.3.1
python-reportlab-2.7-3.3.1
python-reportlab-debugsource-2.7-3.3.1

148746 - SuSE Linux 15.1 openSUSE-SU-2020:0220-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0220-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00069.html

SuSE Linux 15.1
x86_64
python-reportlab-debuginfo-2.7-3.3.1
python-reportlab-2.7-3.3.1
python-reportlab-debugsource-2.7-3.3.1
Description
The scan detected that the host is missing the following update:
SUSE-SU-2020:0372-1

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

SuSE SLES 12 SP4
x86_64
bluez-debuginfo-5.13-5.20.6
libbluetooth3-debuginfo-5.13-5.20.6
bluez-5.13-5.20.6
bluez-debugsource-5.13-5.20.6
libbluetooth3-5.13-5.20.6

SuSE SLES 12 SP5
x86_64
bluez-debuginfo-5.13-5.20.6
libbluetooth3-debuginfo-5.13-5.20.6
bluez-5.13-5.20.6
bluez-debugsource-5.13-5.20.6
libbluetooth3-5.13-5.20.6

SuSE SLED 12 SP4
x86_64
liborcus-0_15-0-0.15.3-10.15.1
libreoffice-officebean-debuginfo-6.3.3.2-43.59.5
libreoffice-librelogo-6.3.3.2-43.59.5
libreoffice-impress-debuginfo-6.3.3.2-43.59.5
libreoffice-base-drivers-postgresql-6.3.3.2-43.59.5
libcmis-0_5-5-0.5.2-9.3.1
libixion-0_15-0-0.15.0-13.12.1
myspell-lightproof-ru_RU-20191016-16.21.1
libreoffice-math-6.3.3.2-43.59.5
libreoffice-pyuno-debuginfo-6.3.3.2-43.59.5
bluez-cups-5.13-5.20.6
myspell-dictionaries-20191016-16.21.1
bluez-cups-debuginfo-5.13-5.20.6
libreoffice-officebean-6.3.3.2-43.59.5
libreoffice-base-6.3.3.2-43.59.5
libreoffice-writer-extensions-6.3.3.2-43.59.5
bluez-debuginfo-5.13-5.20.6
libreoffice-gnome-debuginfo-6.3.3.2-43.59.5
liborcus-debugsource-0.15.3-10.15.1
libreoffice-calc-debuginfo-6.3.3.2-43.59.5
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-20386, CVE-2020-1712

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0208-1

Observation
Updates often remediate critical security problems that should be quickly addressed. For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00055.html

SuSE Linux 15.1
i586
systemd-sysvinit-234-lp151.26.7.1
libudev-devel-234-lp151.26.7.1
libudev-mini1-234-lp151.26.7.1
libsystemd0-mini-234-lp151.26.7.1
nss-systemd-debuginfo-234-lp151.26.7.1
systemd-container-234-lp151.26.7.1
libudev-mini1-debuginfo-234-lp151.26.7.1
systemd-coredump-debuginfo-234-lp151.26.7.1
nss-mymachines-debuginfo-234-lp151.26.7.1
libudev1-debuginfo-234-lp151.26.7.1
systemd-234-lp151.26.7.1
udev-mini-debuginfo-234-lp151.26.7.1
systemd-coredump-234-lp151.26.7.1
udev-234-lp151.26.7.1
systemd-mini-sysvinit-234-lp151.26.7.1
nss-myhostname-debuginfo-234-lp151.26.7.1
nss-systemd-234-lp151.26.7.1
systemd-debgsoure-234-lp151.26.7.1
systemd-mini-debgsoure-234-lp151.26.7.1
systemd-mini-coredump-mini-debuginfo-234-lp151.26.7.1
systemd-mini-debuginfo-234-lp151.26.7.1
systemd-mini-container-mini-234-lp151.26.7.1
systemd-mini-234-lp151.26.7.1
libudev1-234-lp151.26.7.1
systemd-mini-container-mini-debuginfo-234-lp151.26.7.1
systemd-debuginfo-234-lp151.26.7.1
libsystemd0-mini-debuginfo-234-lp151.26.7.1
systemd-logger-234-lp151.26.7.1
systemd-devel-234-lp151.26.7.1
udev-mini-234-lp151.26.7.1
libsystemd0-debuginfo-234-lp151.26.7.1
systemd-container-debuginfo-234-lp151.26.7.1
systemd-mini-coredump-mini-234-lp151.26.7.1
udev-debuginfo-234-lp151.26.7.1
libudev-mini-devel-234-lp151.26.7.1
nss-myhostname-234-lp151.26.7.1
systemd-mini-devel-234-lp151.26.7.1
nss-mymachines-234-lp151.26.7.1
libsystemd0-234-lp151.26.7.1
libudev1-234-lp151.26.7.1
systemd-bash-completion-234-lp151.26.7.1
systemd-mini-bash-completion-234-lp151.26.7.1
noarch
systemd-bash-completion-234-lp151.26.7.1
systemd-mini-bash-completion-234-lp151.26.7.1
148750 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2020:0331-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2020-1712
Description
The scan detected that the host is missing the following update:
SUSE-SU-2020:0331-1

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

SuSE SLED 12 SP4
x86_64
udev-debuginfo-228-150.82.1
systemd-sysvinit-228-150.82.1
udev-228-150.82.1
systemd-debuginfo-228-150.82.1
libudev1-debuginfo-32bit-228-150.82.1
libsystemd0-228-150.82.1
libsystemd0-debuginfo-32bit-228-150.82.1
libudev1-32bit-228-150.82.1
libsystemd0-debuginfo-228-150.82.1
libudev1-228-150.82.1
systemd-228-150.82.1
systemd-debugsource-228-150.82.1
libudev1-debuginfo-228-150.82.1
libsystemd0-debuginfo-32bit-228-150.82.1
libudev1-32bit-228-150.82.1
libsystemd0-debuginfo-228-150.82.1
libudev1-228-150.82.1
libsystemd-228-150.82.1
libsystemd-32bit-228-150.82.1
libsystemd0-32bit-228-150.82.1
noarch
systemd-bash-completion-228-150.82.1

SuSE SLES 12 SP4
noarch
systemd-bash-completion-228-150.82.1

x86_64
udev-debuginfo-228-150.82.1
systemd-sysvinit-228-150.82.1
systemd-debuginfo-228-150.82.1
libudev1-debuginfo-32bit-228-150.82.1
udev-228-150.82.1
libsystemd0-debuginfo-32bit-228-150.82.1
libudev1-32bit-228-150.82.1
libsystemd0-debuginfo-228-150.82.1
libudev1-228-150.82.1
systemd-228-150.82.1
systemd-debugsource-228-150.82.1
libudev1-debuginfo-228-150.82.1
libsystemd0-debuginfo-32bit-228-150.82.1
libudev1-32bit-228-150.82.1
libsystemd0-debuginfo-228-150.82.1
libudev1-228-150.82.1
libsystemd-228-150.82.1
libsystemd-32bit-228-150.82.1
libsystemd0-32bit-228-150.82.1

148751 - SuSE Linux 15.1 openSUSE-SU-2020:0204-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-20372

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0204-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00054.html

SuSE Linux 15.1
x86_64
nginx-debugsource-1.14.2-lp151.4.6.1
nginx-debuginfo-1.14.2-lp151.4.6.1
nginx-1.14.2-lp151.4.6.1
noarch
nginx-source-1.14.2-lp151.4.6.1
vim-plugin-nginx-1.14.2-lp151.4.6.1

148752 - SuSE Linux 15.1 openSUSE-SU-2020:0187-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-1699, CVE-2020-1700

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0187-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00034.html

SuSE Linux 15.1
x86_64
ceph-test-debuginfo-14.2.5.382+g8881d33957-lp151.2.10.1
librgw2-14.2.5.382+g8881d33957-lp151.2.10.1
librados2-14.2.5.382+g8881d33957-lp151.2.10.1
python3-rados-debuginfo-14.2.5.382+g8881d33957-lp151.2.10.1
ceph-resource-agents-14.2.5.382+g8881d33957-lp151.2.10.1
libradosstriper1-14.2.5.382+g8881d33957-lp151.2.10.1
librbd1-14.2.5.382+g8881d33957-lp151.2.10.1
libcephfs2-14.2.5.382+g8881d33957-lp151.2.10.1
python3-rgw-debuginfo-14.2.5.382+g8881d33957-lp151.2.10.1
rbd-fuse-debuginfo-14.2.5.382+g8881d33957-lp151.2.10.1
ceph-mgr-14.2.5.382+g8881d33957-lp151.2.10.1
librgw2-debuginfo-14.2.5.382+g8881d33957-lp151.2.10.1
ceph-mds-14.2.5.382+g8881d33957-lp151.2.10.1
librgw-devel-14.2.5.382+g8881d33957-lp151.2.10.1
ceph-base-14.2.5.382+g8881d33957-lp151.2.10.1
ceph-14.2.5.382+g8881d33957-lp151.2.10.1
rados-objclass-devel-14.2.5.382+g8881d33957-lp151.2.10.1
148753 - SuSE Linux 15.1 openSUSE-SU-2020:0189-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0189-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00036.html

SuSE Linux 15.1
x86_64
chromedriver-debuginfo-80.0.3987.87-lp151.2.63.1
chromedriver-80.0.3987.87-lp151.2.63.1
chromium-debuginfo-80.0.3987.87-lp151.2.63.1
chromium-debugsource-80.0.3987.87-lp151.2.63.1
chromium-80.0.3987.87-lp151.2.63.1

148754 - SuSE SLES 12 SP5 SUSE-SU-2020:0353-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-1712

Description
The scan detected that the host is missing the following update:
SUSE-SU-2020:0353-1

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

SuSE SLES 12 SP5
noarch
systemd-bash-completion-228-157.9.1

x86_64
systemd-debuginfo-32bit-228-157.9.1
libudev1-32bit-228-157.9.1
systemd-32bit-228-157.9.1
libudev1-228-157.9.1
libsystemd0-debuginfo-228-157.9.1
libsystemd0-debuginfo-32bit-228-157.9.1
systemd-228-157.9.1
systemd-debuginfo-228-157.9.1
libsystemd0-228-157.9.1
libudev1-debuginfo-32bit-228-157.9.1
systemd-sysvinit-228-157.9.1
udev-debuginfo-228-157.9.1
libudev1-debuginfo-228-157.9.1
udev-228-157.9.1
libsystemd0-32bit-228-157.9.1
**148756 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2020:0369-1 Update Is Not Installed**

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

**Description**  
The scan detected that the host is missing the following update:  
SUSE-SU-2020:0369-1

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

SuSE SLED 12 SP4  
x86_64  
wicked-debuginfo-0.6.60-2.18.1  
wicked-0.6.60-2.18.1  
wicked-debugsource-0.6.60-2.18.1  
wicked-service-0.6.60-2.18.1

SuSE SLES 12 SP4  
x86_64  
wicked-debuginfo-0.6.60-2.18.1  
wicked-0.6.60-2.18.1  
wicked-debugsource-0.6.60-2.18.1  
wicked-service-0.6.60-2.18.1

**148757 - SuSE Linux 15.1 openSUSE-SU-2020:0207-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes  
Risk Level: High  
CVE: CVE-2019-18903, CVE-2020-7217

**Description**  
The scan detected that the host is missing the following update:  
openSUSE-SU-2020:0207-1

**Observation**  
Updates often remediate critical security problems that should be quickly addressed.  
For more information see:  
https://lists.opensuse.org/opensuse-updates/2020-02/msg00052.html

SuSE Linux 15.1  
x86_64  
wicked-debuginfo-0.6.60-lp151.2.9.1  
wicked-service-0.6.60-lp151.2.9.1  
wicked-0.6.60-lp151.2.9.1  
wicked-debugsource-0.6.60-lp151.2.9.1  
i586
148758 - SuSE Linux 15.1 openSUSE-SU-2020:0213-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0213-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00061.html

SuSE Linux 15.1
i586
pcp-devel-4.3.1-lp151.2.3.1
pcp-pmda-weblog-4.3.1-lp151.2.3.1
pcp-export-zabbix-agent-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-docker-4.3.1-lp151.2.3.1
pcp-pmda-samba-4.3.1-lp151.2.3.1
perl-PCP-LogImport-4.3.1-lp151.2.3.1
libpcp_gui2-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-slurm-4.3.1-lp151.2.3.1
pcp-pmda-news-4.3.1-lp151.2.3.1
python3-pcp-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-cifs-4.3.1-lp151.2.3.1
pcp-export-zabbix-agent-4.3.1-lp151.2.3.1
libpcp_import1-4.3.1-lp151.2.3.1
pcp-pmda-dm-debuginfo-4.3.1-lp151.2.3.1
libpcp_import1-debuginfo-4.3.1-lp151.2.3.1
perl-PCP-LogImport-debuginfo-4.3.1-lp151.2.3.1
pcp-webapi-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-nvidia-gpu-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-ds389log-4.3.1-lp151.2.3.1
libpcp_mmv1-debuginfo-4.3.1-lp151.2.3.1
libpcp_mmv1-4.3.1-lp151.2.3.1
pcp-pmda-logger-4.3.1-lp151.2.3.1
python3-pcp-4.3.1-lp151.2.3.1
pcp-gui-4.3.1-lp151.2.3.1
perl-PCP-PMDA-4.3.1-lp151.2.3.1
pcp-pmda-gpfs-4.3.1-lp151.2.3.1
pcp-pmda-trace-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-dbping-4.3.1-lp151.2.3.1
pcp-pmda-gfs2-4.3.1-lp151.2.3.1
pcp-pmda-activemq-4.3.1-lp151.2.3.1
pcp-pmda-cisco-4.3.1-lp151.2.3.1
pcp-pmda-named-4.3.1-lp151.2.3.1
pcp-debugsource-4.3.1-lp151.2.3.1
pcp-pmda-gluster-4.3.1-lp151.2.3.1
pcp-system-tools-debuginfo-4.3.1-lp151.2.3.1
pcp-export-pcp2elasticsearch-4.3.1-lp151.2.3.1
pcp-pmda-nvidia-gpu-4.3.1-lp151.2.3.1
pcp-pmda-logger-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-json-4.3.1-lp151.2.3.1
pcp-pmda-apache-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-sendmail-4.3.1-lp151.2.3.1
pcp-import-iostat2pcp-4.3.1-lp151.2.3.1
pcp-pmda-elasticsearch-4.3.1-lp151.2.3.1
pcp-export-pcp2json-4.3.1-lp151.2.3.1
libpcp_gui2-4.3.1-lp151.2.3.1
pcp-export-pcp2spark-4.3.1-lp151.2.3.1
pcp-manager-debuginfo-4.3.1-lp151.2.3.1
pcp-manager-4.3.1-lp151.2.3.1
pcp-pmda-vmware-4.3.1-lp151.2.3.1
pcp-zeroconf-4.3.1-lp151.2.3.1
pcp-pmda-docker-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-nginx-4.3.1-lp151.2.3.1
pcp-pmda-bash-4.3.1-lp151.2.3.1
pcp-webapi-4.3.1-lp151.2.3.1
libpcp_trace2-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-pdns-4.3.1-lp151.2.3.1
pcp-pmda-nutcracker-4.3.1-lp151.2.3.1
pcp-pmda-redis-4.3.1-lp151.2.3.1
pcp-pmda-perfevent-4.3.1-lp151.2.3.1
pcp-pmda-infiniband-debuginfo-4.3.1-lp151.2.3.1
perl-PCP-MMV-debuginfo-4.3.1-lp151.2.3.1
libpcp_web1-4.3.1-lp151.2.3.1
pcp-system-tools-4.3.1-lp151.2.3.1
pcp-pmda-cisco-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-systemd-4.3.1-lp151.2.3.1
pcp-pmda-mailq-4.3.1-lp151.2.3.1
pcp-pmda-oracle-4.3.1-lp151.2.3.1
pcp-pmda-infiniband-4.3.1-lp151.2.3.1
pcp-pmda-bonding-4.3.1-lp151.2.3.1
pcp-export-pcp2zabbix-4.3.1-lp151.2.3.1
pcp-pmda-mic-4.3.1-lp151.2.3.1
libpcp-devel-4.3.1-lp151.2.3.1
pcp-import-ganglia2pcp-4.3.1-lp151.2.3.1
pcp-pmda-sendmail-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-gpsd-4.3.1-lp151.2.3.1
pcp-pmda-shping-debuginfo-4.3.1-lp151.2.3.1
perl-PCP-LogSummary-4.3.1-lp151.2.3.1

noarch
pcp-doc-4.3.1-lp151.2.3.1

x86_64
pcp-devel-4.3.1-lp151.2.3.1
pcp-pmda-weblog-4.3.1-lp151.2.3.1
pcp-export-zabbix-agent-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-docker-4.3.1-lp151.2.3.1
pcp-pmda-samba-4.3.1-lp151.2.3.1
perl-PCP-LogImport-4.3.1-lp151.2.3.1
libpcp_gui2-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-slurm-4.3.1-lp151.2.3.1
pcp-pmda-news-4.3.1-lp151.2.3.1
python3-pcp-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-cifs-4.3.1-lp151.2.3.1
pcp-export-zabbix-agent-4.3.1-lp151.2.3.1
libpcp_import1-4.3.1-lp151.2.3.1
pcp-pmda-dm-debuginfo-4.3.1-lp151.2.3.1
libpcp_import1-debuginfo-4.3.1-lp151.2.3.1
perl-PCP-LogImport-debuginfo-4.3.1-lp151.2.3.1
pcp-webapi-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-nvidia-gpu-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-ds389log-4.3.1-lp151.2.3.1
libpcp_mmv1-debuginfo-4.3.1-lp151.2.3.1
libpcp_mmv1-4.3.1-lp151.2.3.1
pcp-pmda-loggr-4.3.1-lp151.2.3.1
python3-pcp-4.3.1-lp151.2.3.1
pcp-gui-4.3.1-lp151.2.3.1
perl-PCP-PMDA-4.3.1-lp151.2.3.1
pcp-pmda-gpfs-4.3.1-lp151.2.3.1
pcp-pmda-trace-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-dbping-4.3.1-lp151.2.3.1
pcp-pmda-gfs2-4.3.1-lp151.2.3.1
pcp-pmda-activemq-4.3.1-lp151.2.3.1
pcp-pmda-cisco-4.3.1-lp151.2.3.1
pcp-pmda-named-4.3.1-lp151.2.3.1
pcp-debugsource-4.3.1-lp151.2.3.1
pcp-pmda-gluster-4.3.1-lp151.2.3.1
pcp-system-tools-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-postfix-4.3.1-lp151.2.3.1
pcp-testsuite-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-perfevent-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-mailq-debuginfo-4.3.1-lp151.2.3.1
perl-PCP-MMV-4.3.1-lp151.2.3.1
pcp-gui-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-mysql-4.3.1-lp151.2.3.1
pcp-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-lustrecomm-debuginfo-4.3.1-lp151.2.3.1
pcp-pmda-nfsclient-4.3.1-lp151.2.3.1

148759 - SuSE Linux 15.1 openSUSE-SU-2020:0219-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-19921

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0219-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00066.html

SuSE Linux 15.1
x86_64
docker-runc-1.0.0rc8+gitr3917_3e425f80a8c9-lp151.3.15.1
docker-runc-debuginfo-1.0.0rc8+gitr3917_3e425f80a8c9-lp151.3.15.1

160676 - CentOS 7 CESA-2020-0366 Update Is Not Installed

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

CentOS 7
x86_64
cernvm-common-release-4.1.8+git2a3f9_1-x86_64-lp151.3.15.1
cernvm-common-debuginfo-4.1.8+git2a3f9_1-x86_64-lp151.3.15.1
Risk Level: High

Description
The scan detected that the host is missing the following update:
CESA-2020-0366

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://lists.centos.org/pipermail/centos-announce/2020-February/035623.html

CentOS 7
x86_64
qemu-img-1.5.3-167.el7_7.4
qemu-kvm-common-1.5.3-167.el7_7.4
qemu-kvm-1.5.3-167.el7_7.4
qemu-kvm-tools-1.5.3-167.el7_7.4

160678 - CentOS 7 CESA-2020-0375 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
CESA-2020-0375

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://lists.centos.org/pipermail/centos-announce/2020-February/035620.html

CentOS 7
x86_64
kernel-debug-3.10.0-1062.12.1.el7
kernel-tools-libs-3.10.0-1062.12.1.el7
kernel-tools-libs-devel-3.10.0-1062.12.1.el7
kernel-debug-devel-3.10.0-1062.12.1.el7
kernel-devel-3.10.0-1062.12.1.el7
python-perf-3.10.0-1062.12.1.el7
kernel-headers-3.10.0-1062.12.1.el7
kernel-tools-3.10.0-1062.12.1.el7
kernel-3.10.0-1062.12.1.el7
bpftool-3.10.0-1062.12.1.el7
perf-3.10.0-1062.12.1.el7
noarch
kernel-abi-whitelists-3.10.0-1062.12.1.el7
kernel-doc-3.10.0-1062.12.1.el7

160679 - CentOS 7 CESA-2019-2079 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
CESA-2019-2079

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://lists.centos.org/pipermail/centos-announce/2020-February/035636.html

CentOS 7
x86_64
xorg-x11-driv-ati-19.0.1-3.el7_7

164115 - Oracle Enterprise Linux ELSA-2020-0339 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High

Description
The scan detected that the host is missing the following update:
ELSA-2020-0339

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009626.html

OEL8
x86_64
kernel-devel-4.18.0-147.5.1.el8_1
kernel-doc-4.18.0-147.5.1.el8_1
kernel-debug-4.18.0-147.5.1.el8_1
kernel-debug-core-4.18.0-147.5.1.el8_1
kernel-modules-extra-4.18.0-147.5.1.el8_1
kernel-debug-modules-4.18.0-147.5.1.el8_1
perf-4.18.0-147.5.1.el8_1
kernel-cross-headers-4.18.0-147.5.1.el8_1
kernel-debug-devel-4.18.0-147.5.1.el8_1
kernel-tools-libs-4.18.0-147.5.1.el8_1
kernel-debug-modules-extra-4.18.0-147.5.1.el8_1
kernel-4.18.0-147.5.1.el8_1
kernel-core-4.18.0-147.5.1.el8_1
bpftool-4.18.0-147.5.1.el8_1
kernel-tools-4.18.0-147.5.1.el8_1
kernel-abi-whitelists-4.18.0-147.5.1.el8_1
kernel-tools-libs-devel-4.18.0-147.5.1.el8_1
kernel-modules-4.18.0-147.5.1.el8_1
164118 - Oracle Enterprise Linux ELSA-2020-0374 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ELSA-2020-0374

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

OEL7
x86_64
kernel-headers-3.10.0-1062.12.1.el7
kernel-3.10.0-1062.12.1.el7
kernel-devel-3.10.0-1062.12.1.el7
kernel-abi-whitelists-3.10.0-1062.12.1.el7
kernel-doc-3.10.0-1062.12.1.el7
python-perf-3.10.0-1062.12.1.el7
kernel-debug-devel-3.10.0-1062.12.1.el7
kernel-debug-3.10.0-1062.12.1.el7
kernel-tools-3.10.0-1062.12.1.el7
kernel-tools-libs-3.10.0-1062.12.1.el7
kernel-tools-libs-devel-3.10.0-1062.12.1.el7
perf-3.10.0-1062.12.1.el7
bpftool-3.10.0-1062.12.1.el7

164119 - Oracle Enterprise Linux ELSA-2020-0366 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ELSA-2020-0366

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009595.html

OEL7
x86_64
qemu-img-1.5.3-167.el7_7.4
qemu-kvm-common-1.5.3-167.el7_7.4
qemu-kvm-1.5.3-167.el7_7.4
164120 - Oracle Enterprise Linux ELSA-2020-5532 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-15916

Description
The scan detected that the host is missing the following update:
ELSA-2020-5532

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009632.html

OEL6
x86_64
kernel-uek-firmware-2.6.39-400.319.1.el6uek
kernel-uek-2.6.39-400.319.1.el6uek
kernel-uek-doc-2.6.39-400.319.1.el6uek
kernel-uek-debug-2.6.39-400.319.1.el6uek
kernel-uek-debug-devel-2.6.39-400.319.1.el6uek
kernel-uek-devel-2.6.39-400.319.1.el6uek

i386
kernel-uek-firmware-2.6.39-400.319.1.el6uek
kernel-uek-doc-2.6.39-400.319.1.el6uek
kernel-uek-2.6.39-400.319.1.el6uek
kernel-uek-debug-2.6.39-400.319.1.el6uek
kernel-uek-debug-devel-2.6.39-400.319.1.el6uek
kernel-uek-devel-2.6.39-400.319.1.el6uek

164121 - Oracle Enterprise Linux ELSA-2020-0378 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ELSA-2020-0378

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009594.html

OEL7
x86_64
python2-ipalib-4.6.5-11.0.1.el7_7.4
ipa-python-compat-4.6.5-11.0.1.el7_7.4
164122 - Oracle Enterprise Linux ELSA-2020-5535 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ELSA-2020-5535

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009635.html
http://oss.oracle.com/pipermail/el-errata/2020-February/009636.html

OEL7
x86_64
kernel-uek-devel-4.1.12-124.36.1.el7uek
kernel-uek-debug-devel-4.1.12-124.36.1.el7uek
kernel-uek-doc-4.1.12-124.36.1.el7uek
kernel-uek-4.1.12-124.36.1.el7uek
kernel-uek-debug-4.1.12-124.36.1.el7uek
kernel-uek-firmware-4.1.12-124.36.1.el7uek

OEL6
x86_64
kernel-uek-debug-4.1.12-124.36.1.el6uek
kernel-uek-debug-devel-4.1.12-124.36.1.el6uek
kernel-uek-doc-4.1.12-124.36.1.el6uek
kernel-uek-devel-4.1.12-124.36.1.el6uek
kernel-uek-firmware-4.1.12-124.36.1.el6uek
kernel-uek-4.1.12-124.36.1.el6uek

171194 - Amazon Linux AMI ALAS-2020-1338 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
ALAS-2020-1338

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

https://alas.aws.amazon.com/ALAS-2020-1338.html

Amazon Linux AMI

kernel-tools-debuginfo-4.14.165-102.185.amzn1
kernel-debuginfo-4.14.165-102.185.amzn1
perf-debuginfo-4.14.165-102.185.amzn1
kernel-headers-4.14.165-102.185.amzn1
kernel-4.14.165-102.185.amzn1
perf-4.14.165-102.185.amzn1
kernel-devel-4.14.165-102.185.amzn1
kernel-tools-devel-4.14.165-102.185.amzn1
kernel-tools-4.14.165-102.185.amzn1
kernel-debuginfo-common-x86_64-4.14.165-102.185.amzn1

i686

kernel-tools-debuginfo-4.14.165-102.185.amzn1
kernel-debuginfo-4.14.165-102.185.amzn1
perf-debuginfo-4.14.165-102.185.amzn1
kernel-headers-4.14.165-102.185.amzn1
kernel-4.14.165-102.185.amzn1
perf-4.14.165-102.185.amzn1
kernel-debuginfo-common-i686-4.14.165-102.185.amzn1
kernel-4.14.165-102.185.amzn1
kernel-devel-4.14.165-102.185.amzn1
kernel-tools-devel-4.14.165-102.185.amzn1
kernel-tools-4.14.165-102.185.amzn1

196595 - Red Hat Enterprise Linux RHSA-2020-0515 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-14868

Description
The scan detected that the host is missing the following update:
RHSA-2020-0515

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


RHEL6D

x86_64
ksh-debuginfo-20120801-38.el6_10
ksh-20120801-38.el6_10

i386
ksh-debuginfo-20120801-38.el6_10
ksh-20120801-38.el6_10

RHEL6S

i386
ksh-debuginfo-20120801-38.el6_10
The scan detected that the host is missing the following update:
RHSA-2020-0514

Updates often remediate critical security problems that should be quickly addressed. For more information see:
196597 - Red Hat Enterprise Linux RHSA-2020-0470 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-2583, CVE-2020-2593, CVE-2020-2604, CVE-2020-2659

Description
The scan detected that the host is missing the following update:
RHSA-2020-0470

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
196598 - Red Hat Enterprise Linux RHSA-2020-0466 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-11745

Description
The scan detected that the host is missing the following update:
RHSA-2020-0466

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

RHEL6_6S
x86_64
nss-softokn-3.14.3-23.el6_6
nss-softokn-devel-3.14.3-23.el6_6
nss-softokn-freebl-devel-3.14.3-23.el6_6
nss-softokn-freebl-3.14.3-23.el6_6
nss-softokn-debuginfo-3.14.3-23.el6_6

196599 - Red Hat Enterprise Linux RHSA-2020-0467 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-2583, CVE-2020-2593, CVE-2020-2604, CVE-2020-2659

Description
The scan detected that the host is missing the following update:
RHSA-2020-0467

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

RHEL6D
x86_64
java-1.7.1-ibm-devel-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-src-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-demo-1.7.1.4.60-1jpp.1.el6_10
i386
java-1.7.1-ibm-devel-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-jdbc-1.7.1.4.60-1jpp.1.el6_10
java-1.7.1-ibm-plugin-1.7.1.4.60-1jpp.1.el6_10
196602 - Red Hat Enterprise Linux RHSA-2020-0468 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-2583, CVE-2020-2593, CVE-2020-2604, CVE-2020-2659

Description
The scan detected that the host is missing the following update:
RHSA-2020-0468

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

RHEL7D
x86_64
java-1.7.1-ibm-src-1.7.1.4.60-1jpp.1.el7
java-1.7.1-ibm-jdbc-1.7.1.4.60-1jpp.1.el7
java-1.7.1-ibm-plugin-1.7.1.4.60-1jpp.1.el7
196603 - Red Hat Enterprise Linux RHSA-2020-0469 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2020-2583, CVE-2020-2593, CVE-2020-2604, CVE-2020-2659

Description
The scan detected that the host is missing the following update:
RHSA-2020-0469

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
26026 - (MSPT-Feb2020) Microsoft Win32k Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0721)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0721

Description
A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Win32k 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.

26027 - (MSPT-Feb2020) Microsoft Win32k Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0720)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0720

Description
A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.
Observation
A vulnerability in some versions of Microsoft Win32k 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0729

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 when a .LNK file is processed. 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0738

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 information disclosure.

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

**26118 - (MSPT-Feb2020) Microsoft Office Online Server Not Validate Origin In Cross-Origin Communications Correctly Spoofing (CVE-2020-0695)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0695

Description
A vulnerability in some versions of Microsoft Office Online Server could lead to spoofing.

Observation
A vulnerability in some versions of Microsoft Office Online Server could lead to spoofing.
The flaw lies in not validate origin in cross-origin communications correctly. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

131523 - Debian Linux 10.0, 9.0 DSA-4618-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9278

Description
The scan detected that the host is missing the following update:
DSA-4618-1

Observation
 Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4618

Debian 9.0
all
libexif12_0.6.21-2+deb9u1
libexif-dev_0.6.21-2+deb9u1

Debian 10.0
all
libexif-doc_0.6.21-5.1+deb10u1
libexif-dev_0.6.21-5.1+deb10u1
libexif12_0.6.21-5.1+deb10u1

148749 - SuSE Linux 15.1 openSUSE-SU-2020:0222-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
openSUSE-SU-2020:0222-1

Observation
 Updates often remediate critical security problems that should be quickly addressed.
For more information see:
https://lists.opensuse.org/opensuse-updates/2020-02/msg00070.html

SuSE Linux 15.1
x86_64
hostapd-debugsource-2.9-lp151.4.3.1
hostapd-2.9-lp151.4.3.1
hostapd-debuginfo-2.9-lp151.4.3.1

160677 - CentOS 6 CESA-2020-0471 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-10893

Description
The scan detected that the host is missing the following update:
CESA-2020-0471

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://lists.centos.org/pipermail/centos-announce/2020-February/035638.html

CentOS 6
x86_64
spice-glib-0.26-8.el6_10.2
spice-gtk-tools-0.26-8.el6_10.2
spice-glib-devel-0.26-8.el6_10.2
spice-gtk-devel-0.26-8.el6_10.2
spice-gtk-python-0.26-8.el6_10.2
spice-gtk-0.26-8.el6_10.2

i686
spice-glib-0.26-8.el6_10.2
spice-gtk-tools-0.26-8.el6_10.2
spice-glib-devel-0.26-8.el6_10.2
spice-gtk-devel-0.26-8.el6_10.2
spice-gtk-python-0.26-8.el6_10.2
spice-gtk-0.26-8.el6_10.2

164116 - Oracle Enterprise Linux ELSA-2020-0471 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-10893

Description
The scan detected that the host is missing the following update:
ELSA-2020-0471

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009631.html

OEL6
x86_64
spice-glib-0.26-8.el6_10.2
spice-gtk-tools-0.26-8.el6_10.2
spice-glib-devel-0.26-8.el6_10.2
spice-gtk-devel-0.26-8.el6_10.2
spice-gtk-python-0.26-8.el6_10.2
spice-gtk-0.26-8.el6_10.2

i386
spice-glib-0.26-8.el6_10.2
183196 - FreeBSD libexif Privilege Escalation (00f30cba-4d23-11ea-86ba-641c67a117d8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9278

Description
The scan detected that the host is missing the following update:
libexif -- privilege escalation (00f30cba-4d23-11ea-86ba-641c67a117d8)

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/00f30cba-4d23-11ea-86ba-641c67a117d8.html

Affected packages:
libexif < 0.6.21_5

196601 - Red Hat Enterprise Linux RHSA-2020-0471 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-10893

Description
The scan detected that the host is missing the following update:
RHSA-2020-0471

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

RHEL6D
x86_64
spice-glib-0.26-8.el6_10.2
spice-gtk-tools-0.26-8.el6_10.2
spice-glib-devel-0.26-8.el6_10.2
spice-gtk-devel-0.26-8.el6_10.2
spice-gtk-python-0.26-8.el6_10.2
spice-gtk-0.26-8.el6_10.2
spice-gtk-debuginfo-0.26-8.el6_10.2

i386
spice-glib-0.26-8.el6_10.2
spice-gtk-tools-0.26-8.el6_10.2
spice-glib-devel-0.26-8.el6_10.2
spice-gtk-devel-0.26-8.el6_10.2
spice-gtk-0.26-8.el6_10.2
26029 - (MSPT-Feb2020) Microsoft Win32k Improperly Provides Kernel Information Information Disclosure (CVE-2020-0717)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0717

Description
A vulnerability in some versions of Microsoft Win32k could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Win32k could lead to information disclosure.

The flaw lies in improperly provides kernel information. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26030 - (MSPT-Feb2020) Microsoft MSRT Improperly Handles Junctions Privilege Escalation (CVE-2020-0733)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Description
A vulnerability in some versions of Microsoft MSRT could lead to privilege escalation.

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

The flaw lies in improperly handles junctions. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

Category: Windows Host Assessment -> Patches and Hotfixes  
(RISK LEVEL: MEDIUM)  
CVE: CVE-2020-0701

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 ClipSVC 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.

Category: Windows Host Assessment -> Patches and Hotfixes  
(RISK LEVEL: MEDIUM)  
CVE: CVE-2020-0727

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

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

The flaw lies in improper handles file operations. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

Category: Windows Host Assessment -> Patches and Hotfixes  
(RISK LEVEL: MEDIUM)  
CVE: CVE-2020-0665

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

The flaw lies in the TGT 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.

26034 - (MSPT-Feb2020) Microsoft Windows WER Privilege Escalation (CVE-2020-0754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0754

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.

26035 - (MSPT-Feb2020) Microsoft Windows WER Privilege Escalation (CVE-2020-0753)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0753

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.

26036 - (MSPT-Feb2020) Microsoft Windows Error Reporting Manager Privilege Escalation (CVE-2020-0678)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0678

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 Manager 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.

**26037 - (MSPT-Feb2020) Microsoft Windows Improperly Handles COM Object Creation Privilege Escalation (CVE-2020-0750)**

*Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)*
*Risk Level: Medium*
*CVE: CVE-2020-0750*

**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 COM object creation. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26038 - (MSPT-Feb2020) Microsoft Windows Improperly Handles COM Object Creation Privilege Escalation (CVE-2020-0749)**

*Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)*
*Risk Level: Medium*
*CVE: CVE-2020-0749*

**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 COM object creation. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26039 - (MSPT-Feb2020) Microsoft Windows Improperly Handles COM Object Creation Privilege Escalation (CVE-2020-0685)**

*Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)*
*Risk Level: Medium*
*CVE: CVE-2020-0685*

**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 COM object creation. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
26040 - (MSPT-Feb2020) Microsoft Wireless Network Manager Improperly Handles Memory Privilege Escalation (CVE-2020-0704)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0704

Description
A vulnerability in some versions of Microsoft Wireless Network Manager could lead to privilege escalation.

Observation
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.

26041 - (MSPT-Feb2020) Microsoft DirectX Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0732)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0732

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

Observation
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.

26042 - (MSPT-Feb2020) Microsoft CNG Improperly Handle Objects In Memory Information Disclosure (CVE-2020-0755)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0755

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

Observation
The flaw lies in improper handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26043 - (MSPT-Feb2020) Microsoft CNG Improperly Handle Objects In Memory Information Disclosure (CVE-2020-0748)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Description
A vulnerability in some versions of Microsoft CNG could lead to information disclosure.

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

The flaw lies in the Improperly Handle Objects In Memory component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26044 - (MSPT-Feb2020) Microsoft CNG Improperly Handle Objects In Memory Information Disclosure (CVE-2020-0756)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0756

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

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

The flaw lies in improperly handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26045 - (MSPT-Feb2020) Microsoft CNG Improperly Handle Objects in Memory Information Disclosure (CVE-2020-0677)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0677

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

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

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26046 - (MSPT-Feb2020) Microsoft CNG Improperly Handle Objects in Memory Information Disclosure (CVE-2020-0676)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0676

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

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26047 - (MSPT-Feb2020) Microsoft CNG Improperly Handle Objects in Memory Information Disclosure (CVE-2020-0675)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0675

**Description**
A vulnerability in some versions of Microsoft CNG could lead to information disclosure.

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

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26048 - (MSPT-Feb2020) Microsoft Windows CLFS Information Disclosure (CVE-2020-0658)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0658

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

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

The flaw lies in the CLFS 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.

**26049 - (MSPT-Feb2020) Microsoft Windows CLFS Privilege Escalation (CVE-2020-0657)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0657

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

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

The flaw lies in the Telephony 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.

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

The flaw lies in the Function Discovery 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.

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

The flaw lies in the Function Discovery 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.

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

The flaw lies in the Function Discovery 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.
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 Function Discovery 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.

26054 - (MSPT-Feb2020) Microsoft Windows GDI Information Disclosure (CVE-2020-0744)

Category: Windows Host Assessment -> Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2020-0744

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.

26055 - (MSPT-Feb2020) Microsoft Windows Graphics Component Privilege Escalation (CVE-2020-0715)

Category: Windows Host Assessment -> Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2020-0715

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.

26056 - (MSPT-Feb2020) Microsoft DirectX Improperly Handles Objects in Memory Information Disclosure (CVE-2020-0714)

Category: Windows Host Assessment -> No Credentials Required
Risk Level: Medium
CVE: CVE-2020-0714

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

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

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26057 - (MSPT-Feb2020) Microsoft DirectX Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0709)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0709

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 user to open a vulnerable website, email or document.

26058 - (MSPT-Feb2020) Microsoft Windows Graphics Privilege Escalation (CVE-2020-0745)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0745

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 user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0746

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 Graphics 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.

**26061 - (MSPT-Feb2020) Microsoft Win32k Improperly Provides Kernel Information Information Disclosure (CVE-2020-0716)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0716

Description
A vulnerability in some versions of Microsoft Win32k could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Win32k could lead to information disclosure.

The flaw lies in improperly provides kernel information. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26067 - (MSPT-Feb2020) Microsoft Windows Win32k Privilege Escalation (CVE-2020-0731)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0731

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

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

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

**26070 - (MSPT-Feb2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-0670)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0670

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.
26071 - (MSPT-Feb2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-0669)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0669

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.

26073 - (MSPT-Feb2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-0668)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0668

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.

26081 - (MSPT-Feb2020) Microsoft Windows Browsers Information Disclosure (CVE-2020-0706)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0706

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

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

The flaw lies in the Browser 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.

26082 - (MSPT-Feb2020) Microsoft Edge Improperly Enforce Cross-Domain Policies Privilege Escalation (CVE-2020-0663)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0663

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.

---

26083 - (MSPT-Feb2020) Microsoft Windows Search Indexer Privilege Escalation (CVE-2020-0666)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0666

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 Search Indexer 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.

---

26084 - (MSPT-Feb2020) Microsoft Windows Search Indexer Privilege Escalation (CVE-2020-0667)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0667

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 Search Indexer 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.

---

26085 - (MSPT-Feb2020) Microsoft Windows Search Indexer Privilege Escalation (CVE-2020-0735)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0735

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 Search Indexer 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.

26086 - (MSPT-Feb2020) Microsoft Search Indexer Privilege Escalation (CVE-2020-0752)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0752

Description
A vulnerability in some versions of Microsoft Search Indexer could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Search Indexer could lead to privilege escalation.

The flaw lies in improperly handle 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.

26087 - (MSPT-Feb2020) Microsoft NDIS Information Disclosure (CVE-2020-0705)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0705

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

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

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26092 - (MSPT-Feb2020) Microsoft Windows Installer MSI Privilege Escalation (CVE-2020-0683)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0683

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

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

The flaw lies in the MSI component. Successful exploitation could allow a local user to gain elevated privileges. The exploit
<table>
<thead>
<tr>
<th>#</th>
<th>(MSPT-Feb2020)</th>
<th>Category: Windows Host Assessment -&gt; Patches and Hotfixes</th>
<th>(CATEGORY REQUIRES CREDENTIALS)</th>
<th>Risk Level: Medium</th>
<th>CVE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>26093</td>
<td><strong>Microsoft Windows Installer MSI Privilege Escalation (CVE-2020-0686)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A vulnerability in some versions of Microsoft Windows Installer could lead to privilege escalation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Observation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A vulnerability in some versions of Microsoft Windows Installer could lead to privilege escalation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The flaw lies in the MSI 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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26094</td>
<td><strong>Microsoft Windows Modules Installer Service Information Disclosure (CVE-2020-0728)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A vulnerability in some versions of Microsoft Windows could lead to information disclosure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Observation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A vulnerability in some versions of Microsoft Windows could lead to information disclosure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The flaw lies in the Modules Installer Service 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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26095</td>
<td><strong>Microsoft Data Sharing Service Privilege Escalation (CVE-2020-0659)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A vulnerability in some versions of Microsoft Data Sharing Service could lead to privilege escalation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Observation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A vulnerability in some versions of Microsoft Data Sharing Service could lead to privilege escalation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The flaw lies in improperly handles file operations. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26096</td>
<td><strong>Microsoft Windows Dssvc.dll Privilege Escalation (CVE-2020-0739)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Level: Medium
CVE: CVE-2020-0739

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 Dssvc.dll 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.

26098 - (MSPT-Feb2020) Microsoft Windows Connected Devices Platform Service Privilege Escalation (CVE-2020-0740)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0740

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 Cdpsvc.dll 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.

26099 - (MSPT-Feb2020) Microsoft Windows Connected Devices Platform Service Privilege Escalation (CVE-2020-0741)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0741

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 Cdpsvc.dll 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.

26100 - (MSPT-Feb2020) Microsoft Windows Connected Devices Platform Service Privilege Escalation (CVE-2020-0742)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0742

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 Cdpsvc.dll 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.

**26101 - (MSPT-Feb2020) Microsoft Windows Connected Devices Platform Service Privilege Escalation (CVE-2020-0743)**
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0743

**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 Cdp.dll 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.

**26102 - (MSPT-Feb2020) Microsoft Backup Service Privilege Escalation (CVE-2020-0703)**
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0703

**Description**
A vulnerability in some versions of Microsoft Backup Service could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Backup Service could lead to privilege escalation.

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

**26103 - (MSPT-Feb2020) Microsoft Windows IME Privilege Escalation (CVE-2020-0707)**
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0707

**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 IME 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.

### 26104 - (MSPT-Feb2020) Microsoft Windows Imaging Library Remote Code Execution (CVE-2020-0708)

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

**Risk Level:** Medium

**CVE:** CVE-2020-0708

**Description**

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

**Observation**

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

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

### 26106 - (MSPT-Feb2020) Microsoft ProfSvc Privilege Escalation (CVE-2020-0730)

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

**Risk Level:** Medium

**CVE:** CVE-2020-0730

**Description**

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

**Observation**

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

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

### 26121 - (MSPT-Feb2020) Microsoft SharePoint Server EWS Privilege Escalation (CVE-2020-0692)

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

**Risk Level:** Medium

**CVE:** CVE-2020-0692

**Description**

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

**Observation**

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

The flaw lies in the EWS component. Successful exploitation could allow a local user to gain elevated privileges.

### 160675 - CentOS 7 CESA-2018-2916 Update Is Not Installed v2
Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15705, CVE-2018-11781

Description
The scan detected that the host is missing the following update:
CESA-2018-2916

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://lists.centos.org/pipermail/centos-announce/2020-February/035628.html

CentOS 7
x86_64
spamassassin-3.4.0-5.el7_7

164114 - Oracle Enterprise Linux ELSA-2020-5533 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
ELSA-2020-5533

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://oss.oracle.com/pipermail/el-errata/2020-February/009627.html

OEL7
x86_64
kernel-uek-tools-4.14.35-1902.10.7.el7uek
kernel-uek-debug-devel-4.14.35-1902.10.7.el7uek
kernel-uek-devel-4.14.35-1902.10.7.el7uek
kernel-uek-4.14.35-1902.10.7.el7uek
kernel-uek-doc-4.14.35-1902.10.7.el7uek
kernel-uek-debug-4.14.35-1902.10.7.el7uek

164117 - Oracle Enterprise Linux ELSA-2020-0335 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-14865

Description
The scan detected that the host is missing the following update:
ELSA-2020-0335
Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2020-February/009624.html

OEL8
x86_64
grub2-tools-2.02-78.0.3.el8_1.1
grub2-efi-aa64-modules-2.02-78.0.3.el8_1.1
grub2-efi-ia32-2.02-78.0.3.el8_1.1
grub2-efi-ia32-cdboot-2.02-78.0.3.el8_1.1
grub2-pc-modules-2.02-78.0.3.el8_1.1
grub2-common-2.02-78.0.3.el8_1.1
grub2-pc-2.02-78.0.3.el8_1.1
grub2-efi-ia32-modules-2.02-78.0.3.el8_1.1
grub2-tools-minimal-2.02-78.0.3.el8_1.1
grub2-tools-extra-2.02-78.0.3.el8_1.1
grub2-efi-x64-modules-2.02-78.0.3.el8_1.1
grub2-efi-x64-cdboot-2.02-78.0.3.el8_1.1
grub2-efi-x64-2.02-78.0.3.el8_1.1
grub2-tools-efi-2.02-78.0.3.el8_1.1

171190 - Amazon Linux AMI ALAS-2020-1340 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium

Description
The scan detected that the host is missing the following update:
ALAS-2020-1340

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

https://alas.aws.amazon.com/ALAS-2020-1340.html

Amazon Linux AMI
noarch
python34-pip-9.0.3-1.27.amzn1
python35-pip-9.0.3-1.27.amzn1
python26-pip-9.0.3-1.27.amzn1
python36-pip-9.0.3-1.27.amzn1
python27-pip-9.0.3-1.27.amzn1

171191 - Amazon Linux AMI ALAS-2020-1342 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-16935

Description
The scan detected that the host is missing the following update:
ALAS-2020-1342
Observation

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


Amazon Linux AMI
x86_64
python36-libs-3.6.10-1.16.amzn1
python35-3.5.7-1.25.amzn1
python36-debuginfo-3.6.10-1.16.amzn1
python36-test-3.6.10-1.16.amzn1
python35-test-3.5.7-1.25.amzn1
python35-tools-3.5.7-1.25.amzn1
python27-2.7.16-1.131.amzn1
python36-tools-3.6.10-1.16.amzn1
python35-libs-3.5.7-1.25.amzn1
python35-debuginfo-3.5.7-1.25.amzn1
python27-test-2.7.16-1.131.amzn1
python27-tools-2.7.16-1.131.amzn1
python27-libs-2.7.16-1.131.amzn1
python36-3.6.10-1.16.amzn1
python36-devel-3.6.10-1.16.amzn1
python35-devel-3.5.7-1.25.amzn1
python27-devel-2.7.16-1.131.amzn1
python27-debuginfo-2.7.16-1.131.amzn1
python36-debug-3.6.10-1.16.amzn1

i686
python36-libs-3.6.10-1.16.amzn1
python35-3.5.7-1.25.amzn1
python36-debuginfo-3.6.10-1.16.amzn1
python36-test-3.6.10-1.16.amzn1
python35-test-3.5.7-1.25.amzn1
python35-tools-3.5.7-1.25.amzn1
python27-2.7.16-1.131.amzn1
python36-tools-3.6.10-1.16.amzn1
python35-libs-3.5.7-1.25.amzn1
python35-debuginfo-3.5.7-1.25.amzn1
python27-test-2.7.16-1.131.amzn1
python27-tools-2.7.16-1.131.amzn1
python27-libs-2.7.16-1.131.amzn1
python36-3.6.10-1.16.amzn1
python36-devel-3.6.10-1.16.amzn1
python35-devel-3.5.7-1.25.amzn1
python27-devel-2.7.16-1.131.amzn1
python27-debuginfo-2.7.16-1.131.amzn1
python36-debug-3.6.10-1.16.amzn1

**171192 - Amazon Linux AMI ALAS-2020-1339 Update Is Not Installed**

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

Description

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

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


Amazon Linux AMI
x86_64

php73-process-7.3.13-1.22.amzn1
php73-fpm-7.3.13-1.22.amzn1
php73-mysqld-7.3.13-1.22.amzn1
php72-json-7.2.26-1.19.amzn1
php72-fpm-7.2.26-1.19.amzn1
php72-gmp-7.2.26-1.19.amzn1
php73-bcmath-7.3.13-1.22.amzn1
php72-xl-7.2.26-1.19.amzn1
php73-common-7.3.13-1.22.amzn1
php73-gmp-7.3.13-1.22.amzn1
php72-mbstring-7.2.26-1.19.amzn1
php73-devel-7.3.13-1.22.amzn1
php72-recode-7.2.26-1.19.amzn1
php73-7.3.13-1.22.amzn1
php72-enchant-7.2.26-1.19.amzn1
php73-enchant-7.3.13-1.22.amzn1
php72-pspell-7.2.26-1.19.amzn1
php73-intl-7.3.13-1.22.amzn1
php72-odbc-7.2.26-1.19.amzn1
php72-debuginfo-7.2.26-1.19.amzn1
php73-xmlrpc-7.3.13-1.22.amzn1
php73-soap-7.3.13-1.22.amzn1
php73-cli-7.3.13-1.22.amzn1
php72-bcmath-7.2.26-1.19.amzn1
php72-dba-7.2.26-1.19.amzn1
php73-pgsql-7.3.13-1.22.amzn1
php73-xl-7.3.13-1.22.amzn1
php73-ldap-7.3.13-1.22.amzn1
php73-dba-7.3.13-1.22.amzn1
php72-common-7.2.26-1.19.amzn1
php72-xmlrpc-7.2.26-1.19.amzn1
php72-pdo-dblib-7.2.26-1.19.amzn1
php73-odbc-7.3.13-1.22.amzn1
php72-7.2.26-1.19.amzn1
php72-pgsql-7.2.26-1.19.amzn1
php73-json-7.3.13-1.22.amzn1
php72-gd-7.2.26-1.19.amzn1
php73-recode-7.3.13-1.22.amzn1
php73-recode-7.3.13-1.22.amzn1
php73-imap-7.3.13-1.22.amzn1
php73-pspell-7.3.13-1.22.amzn1
php72-imap-7.2.26-1.19.amzn1
php72-process-7.2.26-1.19.amzn1
php73-opcache-7.3.13-1.22.amzn1
php72-cli-7.2.26-1.19.amzn1
php73-pdo-7.3.13-1.22.amzn1
php73-embedded-7.3.13-1.22.amzn1
php72-intl-7.2.26-1.19.amzn1
php72-devel-7.2.26-1.19.amzn1
php73-dbg-7.3.13-1.22.amzn1
php72-opcache-7.2.26-1.19.amzn1
php72-ldap-7.2.26-1.19.amzn1
php73-mbstring-7.3.13-1.22.amzn1
php73-debuginfo-7.3.13-1.22.amzn1
php72-ldap-7.2.26-1.19.amzn1
php72-dbg-7.2.26-1.19.amzn1
php72-snmp-7.2.26-1.19.amzn1
php73-snmp-7.3.13-1.22.amzn1
php72-tidy-7.2.26-1.19.amzn1
php72-soap-7.2.26-1.19.amzn1
php72-embedded-7.2.26-1.19.amzn1
php72-pdo-7.2.26-1.19.amzn1
php73-tidy-7.3.13-1.22.amzn1
php73-gd-7.3.13-1.22.amzn1
php73-pdo-dblib-7.3.13-1.22.amzn1

i686
php73-enchant-7.3.13-1.22.amzn1
php73-pspell-7.3.13-1.22.amzn1
php73-fpm-7.3.13-1.22.amzn1
php73-mysqlnd-7.3.13-1.22.amzn1
php72-json-7.2.26-1.19.amzn1
php72-fpm-7.2.26-1.19.amzn1
php73-odbc-7.3.13-1.22.amzn1
php73-bcmath-7.3.13-1.22.amzn1
php72-xmll-7.2.26-1.19.amzn1
php73-common-7.3.13-1.22.amzn1
php73-gmp-7.3.13-1.22.amzn1
php72-mbstring-7.2.26-1.19.amzn1
php73-mbstring-7.3.13-1.22.amzn1
php73-devel-7.3.13-1.22.amzn1
php73-7.3.13-1.22.amzn1
php72-enchant-7.2.26-1.19.amzn1
php72-common-7.2.26-1.19.amzn1
php72-pspell-7.2.26-1.19.amzn1
php73-pgsql-7.3.13-1.22.amzn1
php73-intl-7.3.13-1.22.amzn1
php72-odbc-7.2.26-1.19.amzn1
php72-debuginfo-7.2.26-1.19.amzn1
php73-soap-7.3.13-1.22.amzn1
php73-cli-7.3.13-1.22.amzn1
php72-bcmath-7.2.26-1.19.amzn1
php73-process-7.3.13-1.22.amzn1
php73-xmlrpc-7.3.13-1.22.amzn1
php73-xmll-7.3.13-1.22.amzn1
php72-xmlrpc-7.2.26-1.19.amzn1
php73-ldap-7.3.13-1.22.amzn1
php72-embedded-7.2.26-1.19.amzn1
php72-recode-7.2.26-1.19.amzn1
php72-recode-7.2.26-1.19.amzn1
php72-pdo-dblib-7.2.26-1.19.amzn1
php72-7.2.26-1.19.amzn1
php72-pgsql-7.2.26-1.19.amzn1
php73-json-7.3.13-1.22.amzn1
php72-gd-7.2.26-1.19.amzn1
php73-recode-7.3.13-1.22.amzn1
php73-imap-7.3.13-1.22.amzn1
php73-embedded-7.3.13-1.22.amzn1
php72-dba-7.2.26-1.19.amzn1
php72-process-7.2.26-1.19.amzn1
php73-opcache-7.3.13-1.22.amzn1
php72-cli-7.2.26-1.19.amzn1
**171193 - Amazon Linux AMI ALAS-2020-1341 Update Is Not Installed**

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

Risk Level: Medium


**Description**

The scan detected that the host is missing the following update:
ALAS-2020-1341

**Observation**

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

https://alas.aws.amazon.com/ALAS-2020-1341.html

Amazon Linux AMI
x86_64
spamassassin-3.4.3-2.2.amzn1
spamassassin-debuginfo-3.4.3-2.2.amzn1

i686
spamassassin-3.4.3-2.2.amzn1
spamassassin-debuginfo-3.4.3-2.2.amzn1

**26074 - (MSPT-Feb2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-0713)**

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

Risk Level: Medium

CVE: CVE-2020-0713

**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.

26075 - (MSPT-Feb2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-0712)
Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0712

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.

26076 - (MSPT-Feb2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-0711)
Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0711

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.

26077 - (MSPT-Feb2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-0710)
Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0710

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.

### 131522 - Debian Linux 10.0, 9.0 DSA-4624-1 Update Is Not Installed

**Category:** SSH Module -> NonIntrusive -> Debian Patches and Hotfixes  
**Risk Level:** Medium  
**CVE:** CVE-2017-1000159, CVE-2019-1010006, CVE-2019-11459

**Description**  
The scan detected that the host is missing the following update:  
DSA-4624-1

**Observation**  
Updates often remediate critical security problems that should be quickly addressed.  
For more information see:  
http://www.debian.org/security/2020/dsa-4624

Debian 9.0  
all  
evince_3.22.1-3+deb9u2

Debian 10.0  
all  
evince_3.30.2-3+deb10u1

### 148755 - SuSE Linux 15.1 openSUSE-SU-2020:0214-1 Update Is Not Installed

**Category:** SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes  
**Risk Level:** Medium  
**CVE:** CVE-2018-16471, CVE-2019-16782

**Description**  
The scan detected that the host is missing the following update:  
openSUSE-SU-2020:0214-1

**Observation**  
Updates often remediate critical security problems that should be quickly addressed.  
For more information see:  
https://lists.opensuse.org/opensuse-updates/2020-02/msg00059.html

SuSE Linux 15.1  
x86_64  
ruby2.5-rubygem-rack-doc-2.0.8-lp151.3.3.1  
ruby2.5-rubygem-rack-testsuite-2.0.8-lp151.3.3.1  
ruby2.5-rubygem-rack-2.0.8-lp151.3.3.1

### 131521 - Debian Linux 10.0, 9.0 DSA-4620-1 Update Is Not Installed

**Category:** SSH Module -> NonIntrusive -> Debian Patches and Hotfixes  
**Risk Level:** Low
Description
The scan detected that the host is missing the following update:
DSA-4620-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4620

Debian 9.0
all
firefox-esr_68.5.0esr-1~deb9u1

Debian 10.0
all
firefox-esr_68.5.0esr-1~deb10u1

---

131524 - Debian Linux 10.0 DSA-4623-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2020-1720

Description
The scan detected that the host is missing the following update:
DSA-4623-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4623

Debian 10.0
all
postgresql-11_11.7-0+deb10u1

---

131525 - Debian Linux 9.0 DSA-4621-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
DSA-4621-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4621
Debian 9.0
all
openjdk-8-jdk_8u242-b08-1~deb9u1
openjdk-8-jdk-headless_8u242-b08-1~deb9u1
openjdk-8-jre_8u242-b08-1~deb9u1
openjdk-8-source_8u242-b08-1~deb9u1
openjdk-8-doc_8u242-b08-1~deb9u1
openjdk-8-demo_8u242-b08-1~deb9u1
openjdk-8-db_8u242-b08-1~deb9u1
openjdk-8-jre-zero_8u242-b08-1~deb9u1
openjdk-8-jre-headless_8u242-b08-1~deb9u1

131526 - Debian Linux 10.0, 9.0 DSA-4625-1 Update Is Not Installed

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

Description
The scan detected that the host is missing the following update:
DSA-4625-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4625

Debian 9.0
all
thunderbird_1:68.5.0-1~deb9u1

Debian 10.0
all
thunderbird_1:68.5.0-1~deb10u1

131527 - Debian Linux 10.0, 9.0 DSA-4619-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-17570

Description
The scan detected that the host is missing the following update:
DSA-4619-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4619

Debian 9.0
all
libxmlrpc3-server-java_3.1.3-8+deb9u1
Debian 10.0

libxmlrpc3-common-java_3.1.3-8+deb9u1
libxmlrpc3-client-java_3.1.3-8+deb9u1
libxmlrpc3-java-doc_3.1.3-8+deb9u1

Category: SSH Module -&gt; NonIntrusive -&gt; Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2020-1720

Description
The scan detected that the host is missing the following update:
DSA-4622-1

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.debian.org/security/2020/dsa-4622

Debian 9.0

postgresql-9.6_9.6.17-0+deb9u1

Category: SSH Module -&gt; NonIntrusive -&gt; FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2020-3757

Description
The scan detected that the host is missing the following update:
Flash Player -- arbitrary code execution (d460b640-4cdf-11ea-a59e-6451062f0f7a)

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/d460b640-4cdf-11ea-a59e-6451062f0f7a.html

Affected packages:
linux-flashplayer < 32.0.0.330

Category: SSH Module -&gt; NonIntrusive -&gt; FreeBSD Patches and Hotfixes
Risk Level: Low

CVE-2020-1720

131528 - Debian Linux 9.0 DSA-4622-1 Update Is Not Installed

183188 - FreeBSD Flash Player Arbitrary Code Execution (d460b640-4cdf-11ea-a59e-6451062f0f7a)

183189 - FreeBSD ksh93 Certain Environment Variables Interpreted As Arithmetic Expressions On Startup, Leading To Code Injection (8b20d71)
The scan detected that the host is missing the following update:

### ksh93
- certain environment variables interpreted as arithmetic expressions on startup, leading to code injection (8b20d716-49df-11ea-9f7b-206a8a720317)

#### Observations

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

For more information see:


**Affected packages:**
- ksh93 < 2020.0.1_1
- ksh93-devel < 2020.02.07

---

#### 183190 - FreeBSD FreeBSD Missing IPsec Anti-replay Window Check (5797c807-4279-11ea-b184-f8b156ac3ff9)

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

**Risk Level:** Low

**CVE:** CVE-2019-5613

**Description**

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

FreeBSD -- Missing IPsec anti-replay window check (5797c807-4279-11ea-b184-f8b156ac3ff9)

**Observation**

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

For more information see:


**Affected packages:**
- 12.0 <= FreeBSD-kernel < 12.0_13

---

#### 183191 - FreeBSD FreeBSD Libfetch Buffer Overflow (22b41bc5-4279-11ea-b184-f8b156ac3ff9)

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

**Risk Level:** Low

**CVE:** CVE-2020-7450

**Description**

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

FreeBSD -- libfetch buffer overflow (22b41bc5-4279-11ea-b184-f8b156ac3ff9)

**Observation**

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

For more information see:


**Affected packages:**
- 12.1 <= FreeBSD < 12.1_2
- 12.0 <= FreeBSD < 12.0_13
11.3 <= FreeBSD < 11.3.6

**183192 - FreeBSD grub2-bhyve Multiple Privilege Escalations (9d6a48a7-4dad-11ea-8a1d-7085c25400ea)**

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:
grub2-bhyve -- multiple privilege escalations (9d6a48a7-4dad-11ea-8a1d-7085c25400ea)

**Observation**
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/9d6a48a7-4dad-11ea-8a1d-7085c25400ea.html

Affected packages:
grub2-bhyve < 0.40_8

**183193 - FreeBSD dovecot Multiple Vulnerabilities (74db0d02-b140-4c32-aac6-1f1e81e1ad30)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2020-7046, CVE-2020-7967

**Description**
The scan detected that the host is missing the following update:
dovecot -- multiple vulnerabilities (74db0d02-b140-4c32-aac6-1f1e81e1ad30)

**Observation**
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/74db0d02-b140-4c32-aac6-1f1e81e1ad30.html

Affected packages:
dovecot < 2.3.9.3

**183194 - FreeBSD Gitlab Vulnerability (1ece5591-4ea9-11ea-86f0-001b217b3468)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2020-8795

**Description**
The scan detected that the host is missing the following update:
Gitlab -- Vulnerability (1ece5591-4ea9-11ea-86f0-001b217b3468)

**Observation**
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
Affected packages:
12.7.0 <= gitlab-ce < 12.7.6
12.6.0 <= gitlab-ce < 12.6.7
12.5.0 <= gitlab-ce < 12.5.10

183195 - FreeBSD NGINX HTTP Request Smuggling (c1202de8-4b29-11ea-9673-4c72b94353b5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-20372

Description
The scan detected that the host is missing the following update:
NGINX -- HTTP request smuggling (c1202de8-4b29-11ea-9673-4c72b94353b5)

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/c1202de8-4b29-11ea-9673-4c72b94353b5.html

Affected packages:
nginx < 1.16.1.11.2
nginx-devel < 1.17.7

183197 - FreeBSD clamav Denial-of-Service (DoS) vulnerability (e7bc2b99-485a-11ea-bff9-9c5c8e75236a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2020-3123

Description
The scan detected that the host is missing the following update:
clamav -- Denial-of-Service (DoS) vulnerability (e7bc2b99-485a-11ea-bff9-9c5c8e75236a)

Observation
Updates often remediate critical security problems that should be quickly addressed.
For more information see:
http://www.vuxml.org/freebsd/e7bc2b99-485a-11ea-bff9-9c5c8e75236a.html

Affected packages:
clamav < 0.102.2,1

183198 - FreeBSD FreeBSD Kernel Stack Data Disclosure (6025d173-4279-11ea-b184-f8b156ac3ff9)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-15875

Description
The scan detected that the host is missing the following update:
FreeBSD -- kernel stack data disclosure (6025d173-4279-11ea-b184-f8b156ac3ff9)

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


Affected packages:
12.1 <= FreeBSD-kernel < 12.1_2
12.0 <= FreeBSD-kernel < 12.0_13
11.3 <= FreeBSD-kernel < 11.3_6

**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.

**25189 - IBM WebSphere Application Server Liberty Multiple Vulnerabilities (ibm10883126)**

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

**Update Details**
Observation is updated

**HOW TO UPDATE**

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

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

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

**MCAFEE TECHNICAL SUPPORT**

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

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

Copyright 2020 McAfee, Inc.