2019-APR-10
FSL version 7.6.105

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

195001 - Fedora Linux 28 FEDORA-2019-65c6d11eba Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16880, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-65c6d11eba

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 28

kernel-headers-5.0.6-100.fc28
kernel-tools-5.0.6-100.fc28
kernel-5.0.6-100.fc28

24964 - (MSPT-Apr2019) Microsoft Windows GDI Remote Code Execution (CVE-2019-0853)

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

Risk Level: High

CVE: CVE-2019-0853

Description

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

Observation

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

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

25000 - (MSPT-Apr2019) Microsoft IOleCvt interface Remote Code Execution Vulnerability (CVE-2019-0845)

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

Risk Level: High

CVE: CVE-2019-0845

Description

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

Observation

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

The flaw lies in the iolecvt interface 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.

25028 - (APSB19-17) Multiple Vulnerabilities In Adobe Acrobat And Reader

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

Risk Level: High

CVE: CVE-2019-7061, CVE-2019-7088, CVE-2019-7109, CVE-2019-7110, CVE-2019-7111, CVE-2019-7112, CVE-2019-7113, CVE-2019-7114, CVE-2019-7115, CVE-2019-7116, CVE-2019-7117, CVE-2019-7118, CVE-2019-7119, CVE-2019-7120, CVE-2019-7121, CVE-2019-7122, CVE-2019-7123, CVE-2019-7124, CVE-2019-7125, CVE-2019-7127, CVE-2019-7128

Description

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

Observation

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

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

The update provided by Adobe bulletin APSB19-17 resolves these issues.

25029 - (APSB19-19) Multiple Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2019-7096, CVE-2019-7108

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

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

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in the Adobe Flash Player Runtime. Successful exploitation could allow an attacker to execute remote code and take control of the affected system.

195014 - Fedora Linux 28 FEDORA-2019-3348cb4934 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3348cb4934

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

libssh2-1.8.1-1.fc28

195017 - Fedora Linux 30 FEDORA-2019-70a9d4f970 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
FEDORA-2019-70a9d4f970

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 30

libssh2-1.8.2-1.fc30

24922 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1610)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1610

Description

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

Observation

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

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to improper validation of arguments passed to certain CLI commands. Successful exploitation could allow an authenticated local attacker to gain elevated privileges and execute

arbitrary code on the target system.

24933 - (MSPT-Apr2019) Microsoft SharePoint Cross-Site-Scripting Vulnerability (CVE-2019-0830)

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

Risk Level: High

CVE: CVE-2019-0830

Description

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

Observation

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

The flaw is due to improper handling of a specially crafted web request. Successful exploitation could allow an attacker to perform cross-site scripting attacks.

24938 - (MSPT-Apr2019) Microsoft Edge Chakra Scripting Engine Remote Code Execution (CVE-2019-0806)

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

Risk Level: High

CVE: CVE-2019-0806

Description

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

Observation

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

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

24940 - (MSPT-Apr2019) Microsoft Edge Improperly Handle Objects In Memory Remote Code Execution (CVE-2019-0739)

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

Risk Level: High

CVE: CVE-2019-0739

Description

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

Observation

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

The flaw lies due to improperly 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.

24941 - (MSPT-Apr2019) Microsoft Edge Chakra Scripting Remote Code Execution (CVE-2019-0860)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2019-0860

Description

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

Observation

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

The flaw lies in the chakra scripting 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.

24942 - (MSPT-Apr2019) Microsoft Edge Chakra Scripting Remote Code Execution (CVE-2019-0861)

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

Risk Level: High

CVE: CVE-2019-0861

Description

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

Observation

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

The flaw lies in the chakra scripting 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.

24945 - (MSPT-Apr2019) Microsoft Internet Explorer Improperly Handle Objects In Memory Remote Code Execution (CVE-2019-0752)

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

Risk Level: High

CVE: CVE-2019-0752

Description

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

Observation

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

The flaw lies due to improperly 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.

24946 - (MSPT-Apr2019) Microsoft Internet Explorer Improperly Handle Objects In Memory Remote Code Execution (CVE-2019-0753)

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

Risk Level: High

CVE: CVE-2019-0753

Description

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

Observation

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

The flaw lies due to improperly 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.

24949 - (MSPT-Apr2019) Microsoft Excel Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0828)

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

Risk Level: High

CVE: CVE-2019-0828

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 due to improperly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24950 - (MSPT-Apr2019) Microsoft Office Access Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0823)

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

Risk Level: High

CVE: CVE-2019-0823

Description

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

Observation

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

The flaw lies due to 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.

24951 - (MSPT-Apr2019) Microsoft Office Access Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0826)

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

Risk Level: High

CVE: CVE-2019-0826

Description

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

Observation

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

The flaw lies due to 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.

24952 - (MSPT-Apr2019) Microsoft Office Improperly Handle Files Remote Code Execution (CVE-2019-0801)

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

Risk Level: High

CVE: CVE-2019-0801

Description

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

Observation

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

The flaw lies due to improperly handle files. 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.

24953 - (MSPT-Apr2019) Microsoft Office Access Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0827)

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

Risk Level: High

CVE: CVE-2019-0827

Description

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

Observation

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

The flaw lies due to 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.

24954 - (MSPT-Apr2019) Microsoft Office Access Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0824)

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

Risk Level: High

CVE: CVE-2019-0824

Description

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

Observation

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

The flaw lies due to 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.

24955 - (MSPT-Apr2019) Microsoft Office Access Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0825)

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

Risk Level: High

CVE: CVE-2019-0825

Description

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

Observation

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

The flaw lies due to 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.

24956 - (MSPT-Apr2019) Azure DevOps Server Spoofing Vulnerability (CVE-2019-0857)

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

Risk Level: High

CVE: CVE-2019-0857

Description

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to spoofing.

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

24958 - (MSPT-Apr2019) Microsoft ASP.NET Core Denial of Service (CVE-2019-0815)

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

Risk Level: High

CVE: CVE-2019-0815

Description

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

Observation

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

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

24959 - (MSPT-Apr2019) Microsoft SMB Server Privilege Escalation (CVE-2019-0786)

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

Risk Level: High

CVE: CVE-2019-0786

Description

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

Observation

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

The flaw is due to improper handling of specially crafted files. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24961 - (MSPT-Apr2019) Microsoft Windows Remote Code Execution (CVE-2019-0856)

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

Risk Level: High

CVE: CVE-2019-0856

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

24962 - (MSPT-Apr2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-0859)

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

Risk Level: High

CVE: CVE-2019-0859

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

24963 - (MSPT-Apr2019) Microsoft Windows CSRSS Privilege Escalation (CVE-2019-0735)

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

Risk Level: High

CVE: CVE-2019-0735

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

24966 - (MSPT-Apr2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-0803)

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

Risk Level: High

CVE: CVE-2019-0803

Description

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

Observation

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

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

24969 - (MSPT-Apr2019) Microsoft MSXML Improperly Processes User Input Remote Code Execution (CVE-2019-0794)

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

Risk Level: High

CVE: CVE-2019-0794

Description

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

Observation

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

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

24974 - (MSPT-Apr2019) Microsoft MSXML Improperly Processes User Input Remote Code Execution (CVE-2019-0793)

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

Risk Level: High

CVE: CVE-2019-0793

Description

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

Observation

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

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

24975 - (MSPT-Apr2019) Microsoft MSXML Improperly Processes User Input Remote Code Execution (CVE-2019-0792)

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

Risk Level: High

CVE: CVE-2019-0792

Description

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

Observation

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

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

24976 - (MSPT-Apr2019) Microsoft MSXML Improperly Processes User Input Remote Code Execution (CVE-2019-0791)

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

Risk Level: High

CVE: CVE-2019-0791

Description

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

Observation

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

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

24977 - (MSPT-Apr2019) Microsoft MSXML Improperly Processes User Input Remote Code Execution (CVE-2019-0795)

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

Risk Level: High

CVE: CVE-2019-0795

Description

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

Observation

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

The flaw lies due to improperly processes user input. Successful exploitation by a remote attacker could result in the execution of

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

24978 - (MSPT-Apr2019) Microsoft MSXML Improperly Processes User Input Remote Code Execution (CVE-2019-0790)

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

Risk Level: High

CVE: CVE-2019-0790

Description

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

Observation

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

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

24983 - (MSPT-Apr2019) Microsoft Browsers Improperly Validate Input Remote Code Execution (CVE-2019-0764)

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

Risk Level: High

CVE: CVE-2019-0764

Description

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

Observation

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

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

24984 - (MSPT-Apr2019) Microsoft VBScript Improperly Handle Objects In Memory Remote Code Execution (CVE-2019-0862)

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

Risk Level: High

CVE: CVE-2019-0862

Description

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

Observation

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

The flaw lies due to 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.

24985 - (MSPT-Apr2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0846)

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

Risk Level: High

CVE: CVE-2019-0846

Description

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

Observation

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

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

24986 - (MSPT-Apr2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0847)

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

Risk Level: High

CVE: CVE-2019-0847

Description

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

Observation

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

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

24987 - (MSPT-Apr2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0851)

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

Risk Level: High

CVE: CVE-2019-0851

Description

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

Observation

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

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

24990 - (MSPT-Apr2019) Microsoft VBScript Improperly Handle Objects In Memory Remote Code Execution (CVE-2019-0842)

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

Risk Level: High

CVE: CVE-2019-0842

Description

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

Observation

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

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

25001 - (MSPT-Apr2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0877)

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

Risk Level: High

CVE: CVE-2019-0877

Description

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

Observation

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

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

25014 - (MSPT-Apr2019) Azure DevOps Server Cross-site Scripting Vulnerability (CVE-2019-0874)

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

Risk Level: High

CVE: CVE-2019-0874

Description

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to spoofing.

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

25024 - (MSPT-Apr2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0879)

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

Risk Level: High

CVE: CVE-2019-0879

Description

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

Observation

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

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

131327 - Debian Linux 9.0 DSA-4423-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9894, CVE-2019-9895, CVE-2019-9897, CVE-2019-9898

Description

The scan detected that the host is missing the following update:
DSA-4423-1

Observation

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

http://www.debian.org/security/2019/dsa-4423

Debian 9.0
all
putty_0.67-3+deb9u1

147794 - SuSE Linux 15.0 openSUSE-SU-2019:1148-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6977, CVE-2019-6978

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1148-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00056.html

SuSE Linux 15.0
x86_64
libgd3-debuginfo-2.2.5-lp150.8.1
gd-devel-2.2.5-lp150.8.1
gd-2.2.5-lp150.8.1
gd-debuginfo-2.2.5-lp150.8.1
libgd3-32bit-2.2.5-lp150.8.1
libgd3-2.2.5-lp150.8.1
gd-debugsource-2.2.5-lp150.8.1
libgd3-32bit-debuginfo-2.2.5-lp150.8.1

i586
libgd3-debuginfo-2.2.5-lp150.8.1
gd-devel-2.2.5-lp150.8.1
gd-2.2.5-lp150.8.1

gd-debuginfo-2.2.5-lp150.8.1
libgd3-2.2.5-lp150.8.1
gd-debugsource-2.2.5-lp150.8.1

147796 - SuSE Linux 15.0 openSUSE-SU-2019:1172-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12181, CVE-2019-0160

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1172-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00091.html

SuSE Linux 15.0
i586
ovmf-2017+git1510945757.b2662641d5-lp150.4.16.1
ovmf-tools-2017+git1510945757.b2662641d5-lp150.4.16.1

noarch
qemu-ovmf-ia32-2017+git1510945757.b2662641d5-lp150.4.16.1
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-lp150.4.16.1

x86_64
qemu-ovmf-x86_64-debug-2017+git1510945757.b2662641d5-lp150.4.16.1
ovmf-tools-2017+git1510945757.b2662641d5-lp150.4.16.1
ovmf-2017+git1510945757.b2662641d5-lp150.4.16.1

147799 - SuSE Linux 42.3 openSUSE-SU-2019:1158-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1158-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00072.html

SuSE Linux 42.3
x86_64
ntp-debugsource-4.2.8p13-31.9.1
ntp-4.2.8p13-31.9.1
ntp-doc-4.2.8p13-31.9.1
ntp-debuginfo-4.2.8p13-31.9.1

i586
ntp-debugsource-4.2.8p13-31.9.1
ntp-4.2.8p13-31.9.1
ntp-doc-4.2.8p13-31.9.1
ntp-debuginfo-4.2.8p13-31.9.1

147802 - SuSE Linux 42.3 openSUSE-SU-2019:1178-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9924

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1178-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00093.html

SuSE Linux 42.3
i586
bash-debugsource-4.3-83.15.1
bash-devel-4.3-83.15.1
libreadline6-6.3-83.15.1
libreadline6-debuginfo-6.3-83.15.1
bash-loadables-debuginfo-4.3-83.15.1
bash-loadables-4.3-83.15.1
bash-4.3-83.15.1
bash-debuginfo-4.3-83.15.1
readline-devel-6.3-83.15.1

noarch
bash-doc-4.3-83.15.1
bash-lang-4.3-83.15.1
readline-doc-6.3-83.15.1

x86_64
bash-debuginfo-32bit-4.3-83.15.1
bash-4.3-83.15.1
bash-devel-4.3-83.15.1
readline-devel-6.3-83.15.1
libreadline6-debuginfo-32bit-6.3-83.15.1
libreadline6-32bit-6.3-83.15.1
bash-loadables-4.3-83.15.1
bash-debuginfo-4.3-83.15.1
libreadline6-6.3-83.15.1
readline-devel-32bit-6.3-83.15.1
bash-loadables-debuginfo-4.3-83.15.1
bash-debugsource-4.3-83.15.1
libreadline6-debuginfo-6.3-83.15.1

147804 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0900-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0900-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005310.html

SuSE SLES 12 SP3
x86_64
dovecot22-backend-pgsql-2.2.31-19.14.2
dovecot22-backend-mysql-debuginfo-2.2.31-19.14.2
dovecot22-backend-pgsql-debuginfo-2.2.31-19.14.2
dovecot22-backend-sqlite-debuginfo-2.2.31-19.14.2
dovecot22-2.2.31-19.14.2
dovecot22-debuginfo-2.2.31-19.14.2
dovecot22-backend-mysql-2.2.31-19.14.2
dovecot22-backend-sqlite-2.2.31-19.14.2
dovecot22-debugsource-2.2.31-19.14.2

SuSE SLES 12 SP4
x86_64
dovecot22-backend-pgsql-2.2.31-19.14.2
dovecot22-backend-mysql-debuginfo-2.2.31-19.14.2
dovecot22-backend-pgsql-debuginfo-2.2.31-19.14.2
dovecot22-backend-sqlite-debuginfo-2.2.31-19.14.2
dovecot22-2.2.31-19.14.2
dovecot22-debuginfo-2.2.31-19.14.2
dovecot22-backend-mysql-2.2.31-19.14.2
dovecot22-backend-sqlite-2.2.31-19.14.2
dovecot22-debugsource-2.2.31-19.14.2

147805 - SuSE Linux 42.3 openSUSE-SU-2019:1140-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6977, CVE-2019-6978

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1140-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00064.html

SuSE Linux 42.3
x86_64
gd-debuginfo-32bit-2.1.0-30.1

gd-32bit-2.1.0-30.1
gd-debuginfo-2.1.0-30.1
gd-devel-2.1.0-30.1
gd-debugsource-2.1.0-30.1
gd-2.1.0-30.1

i586
gd-devel-2.1.0-30.1
gd-debuginfo-2.1.0-30.1
gd-debugsource-2.1.0-30.1
gd-2.1.0-30.1

147807 - SuSE Linux 42.3 openSUSE-SU-2019:1152-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1152-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00057.html

SuSE Linux 42.3
x86_64
MozillaThunderbird-translations-other-60.6.1-89.1
MozillaThunderbird-translations-common-60.6.1-89.1
MozillaThunderbird-debugsource-60.6.1-89.1
MozillaThunderbird-60.6.1-89.1
MozillaThunderbird-debuginfo-60.6.1-89.1
MozillaThunderbird-buildsymbols-60.6.1-89.1

147808 - SuSE Linux 15.0 openSUSE-SU-2019:1143-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1143-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00065.html

SuSE Linux 15.0
x86_64
ntp-debuginfo-4.2.8p13-lp150.8.1

ntp-debugsource-4.2.8p13-lp150.8.1
ntp-4.2.8p13-lp150.8.1
ntp-doc-4.2.8p13-lp150.8.1

i586
ntp-debuginfo-4.2.8p13-lp150.8.1
ntp-debugsource-4.2.8p13-lp150.8.1
ntp-4.2.8p13-lp150.8.1
ntp-doc-4.2.8p13-lp150.8.1

147811 - SuSE Linux 15.0 openSUSE-SU-2019:1160-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11410, CVE-2018-11440, CVE-2018-11577, CVE-2018-11683, CVE-2018-11684, CVE-2018-11685, CVE-2018-12085, CVE-2018-17294

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1160-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00076.html

SuSE Linux 15.0
x86_64
liblouis-tools-debuginfo-3.3.0-lp150.3.3.1
liblouis14-debuginfo-3.3.0-lp150.3.3.1
liblouis-tools-3.3.0-lp150.3.3.1
liblouis-doc-3.3.0-lp150.3.3.1
liblouis-devel-3.3.0-lp150.3.3.1
python3-louis-3.3.0-lp150.3.3.1
liblouis-data-3.3.0-lp150.3.3.1
liblouis-debuginfo-3.3.0-lp150.3.3.1
liblouis14-3.3.0-lp150.3.3.1
liblouis-debugsource-3.3.0-lp150.3.3.1

147820 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0897-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-1787, CVE-2019-1788, CVE-2019-1789

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0897-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005308.html

SuSE SLED 12 SP3
x86_64
clamav-debuginfo-0.100.3-33.21.1
clamav-0.100.3-33.21.1
clamav-debugsource-0.100.3-33.21.1

SuSE SLED 12 SP4
x86_64
clamav-debuginfo-0.100.3-33.21.1
clamav-0.100.3-33.21.1
clamav-debugsource-0.100.3-33.21.1

SuSE SLES 12 SP4
x86_64
clamav-debuginfo-0.100.3-33.21.1
clamav-0.100.3-33.21.1
clamav-debugsource-0.100.3-33.21.1

SuSE SLES 12 SP3
x86_64
clamav-debuginfo-0.100.3-33.21.1
clamav-0.100.3-33.21.1
clamav-debugsource-0.100.3-33.21.1

147825 - SuSE SLES 11 SP4 SUSE-SU-2019:14013-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20783, CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024, CVE-2019-9637, CVE-2019-9638, CVE-2019-9639, CVE-2019-9640, CVE-2019-9641, CVE-2019-9675

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:14013-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005304.html

SuSE SLES 11 SP4
i586
php53-xsl-5.3.17-112.58.1
php53-iconv-5.3.17-112.58.1
php53-sysvshm-5.3.17-112.58.1
php53-calendar-5.3.17-112.58.1
apache2-mod_php53-5.3.17-112.58.1
php53-gmp-5.3.17-112.58.1
php53-tokenizer-5.3.17-112.58.1
php53-pspell-5.3.17-112.58.1
php53-curl-5.3.17-112.58.1
php53-dom-5.3.17-112.58.1
php53-bz2-5.3.17-112.58.1
php53-pcntl-5.3.17-112.58.1
php53-intl-5.3.17-112.58.1
php53-shmop-5.3.17-112.58.1
php53-5.3.17-112.58.1

php53-pdo-5.3.17-112.58.1
php53-zlib-5.3.17-112.58.1
php53-gettext-5.3.17-112.58.1
php53-openssl-5.3.17-112.58.1
php53-json-5.3.17-112.58.1
php53-zip-5.3.17-112.58.1
php53-bcmath-5.3.17-112.58.1
php53-sysvsem-5.3.17-112.58.1
php53-mbstring-5.3.17-112.58.1
php53-sysvmsg-5.3.17-112.58.1
php53-gd-5.3.17-112.58.1
php53-mysql-5.3.17-112.58.1
php53-xmlwriter-5.3.17-112.58.1
php53-mcrypt-5.3.17-112.58.1
php53-fileinfo-5.3.17-112.58.1
php53-exif-5.3.17-112.58.1
php53-snmp-5.3.17-112.58.1
php53-wddx-5.3.17-112.58.1
php53-pear-5.3.17-112.58.1
php53-ftp-5.3.17-112.58.1
php53-suhosin-5.3.17-112.58.1
php53-soap-5.3.17-112.58.1
php53-ldap-5.3.17-112.58.1
php53-xmlreader-5.3.17-112.58.1
php53-xmlrpc-5.3.17-112.58.1
php53-pgsql-5.3.17-112.58.1
php53-ctype-5.3.17-112.58.1
php53-dba-5.3.17-112.58.1
php53-fastcgi-5.3.17-112.58.1
php53-odbc-5.3.17-112.58.1

x86_64
php53-xsl-5.3.17-112.58.1
php53-iconv-5.3.17-112.58.1
php53-sysvshm-5.3.17-112.58.1
php53-calendar-5.3.17-112.58.1
apache2-mod_php53-5.3.17-112.58.1
php53-gmp-5.3.17-112.58.1
php53-tokenizer-5.3.17-112.58.1
php53-pspell-5.3.17-112.58.1
php53-curl-5.3.17-112.58.1
php53-dom-5.3.17-112.58.1
php53-bz2-5.3.17-112.58.1
php53-pcntl-5.3.17-112.58.1
php53-intl-5.3.17-112.58.1
php53-shmop-5.3.17-112.58.1
php53-5.3.17-112.58.1
php53-pdo-5.3.17-112.58.1
php53-zlib-5.3.17-112.58.1
php53-gettext-5.3.17-112.58.1
php53-openssl-5.3.17-112.58.1
php53-json-5.3.17-112.58.1
php53-zip-5.3.17-112.58.1
php53-bcmath-5.3.17-112.58.1
php53-sysvsem-5.3.17-112.58.1
php53-mbstring-5.3.17-112.58.1
php53-sysvmsg-5.3.17-112.58.1
php53-gd-5.3.17-112.58.1
php53-mysql-5.3.17-112.58.1
php53-xmlwriter-5.3.17-112.58.1

php53-mcrypt-5.3.17-112.58.1
php53-fileinfo-5.3.17-112.58.1
php53-exif-5.3.17-112.58.1
php53-snmp-5.3.17-112.58.1
php53-wddx-5.3.17-112.58.1
php53-pear-5.3.17-112.58.1
php53-ftp-5.3.17-112.58.1
php53-suhosin-5.3.17-112.58.1
php53-soap-5.3.17-112.58.1
php53-ldap-5.3.17-112.58.1
php53-xmlreader-5.3.17-112.58.1
php53-xmlrpc-5.3.17-112.58.1
php53-pgsql-5.3.17-112.58.1
php53-ctype-5.3.17-112.58.1
php53-dba-5.3.17-112.58.1
php53-fastcgi-5.3.17-112.58.1
php53-odbc-5.3.17-112.58.1

147826 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0878-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0878-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005296.html

SuSE SLES 12 SP3
noarch
apache2-doc-2.4.23-29.40.1

x86_64
apache2-utils-debuginfo-2.4.23-29.40.1
apache2-2.4.23-29.40.1
apache2-prefork-debuginfo-2.4.23-29.40.1
apache2-debugsource-2.4.23-29.40.1
apache2-prefork-2.4.23-29.40.1
apache2-debuginfo-2.4.23-29.40.1
apache2-example-pages-2.4.23-29.40.1
apache2-worker-debuginfo-2.4.23-29.40.1
apache2-utils-2.4.23-29.40.1
apache2-worker-2.4.23-29.40.1

SuSE SLES 12 SP4
noarch
apache2-doc-2.4.23-29.40.1

x86_64
apache2-utils-debuginfo-2.4.23-29.40.1
apache2-2.4.23-29.40.1
apache2-prefork-debuginfo-2.4.23-29.40.1

apache2-debugsource-2.4.23-29.40.1
apache2-prefork-2.4.23-29.40.1
apache2-debuginfo-2.4.23-29.40.1
apache2-example-pages-2.4.23-29.40.1
apache2-worker-debuginfo-2.4.23-29.40.1
apache2-utils-2.4.23-29.40.1
apache2-worker-2.4.23-29.40.1

163839 - Oracle Enterprise Linux ELSA-2019-4600 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10877, CVE-2018-10879, CVE-2018-10881, CVE-2018-10882, CVE-2019-3701

Description

The scan detected that the host is missing the following update:
ELSA-2019-4600

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008627.html
http://oss.oracle.com/pipermail/el-errata/2019-April/008626.html

OEL7
x86_64
kernel-uek-firmware-3.8.13-118.32.1.el7uek
kernel-uek-debug-3.8.13-118.32.1.el7uek
kernel-uek-doc-3.8.13-118.32.1.el7uek
kernel-uek-debug-devel-3.8.13-118.32.1.el7uek
kernel-uek-3.8.13-118.32.1.el7uek
dtrace-modules-3.8.13-118.32.1.el7uek-0.4.5-3.el7
kernel-uek-devel-3.8.13-118.32.1.el7uek

OEL6
x86_64
kernel-uek-devel-3.8.13-118.32.1.el6uek
kernel-uek-firmware-3.8.13-118.32.1.el6uek
dtrace-modules-3.8.13-118.32.1.el6uek-0.4.5-3.el6
kernel-uek-debug-devel-3.8.13-118.32.1.el6uek
kernel-uek-debug-3.8.13-118.32.1.el6uek
kernel-uek-3.8.13-118.32.1.el6uek
kernel-uek-doc-3.8.13-118.32.1.el6uek

171088 - Amazon Linux AMI ALAS-2019-1189 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0211

Description

The scan detected that the host is missing the following update:
ALAS-2019-1189

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1189.html

Amazon Linux AMI
i686
mod24_proxy_html-2.4.39-1.87.amzn1
mod24_md-2.4.39-1.87.amzn1
mod24_ssl-2.4.39-1.87.amzn1
httpd24-2.4.39-1.87.amzn1
httpd24-devel-2.4.39-1.87.amzn1
mod24_ldap-2.4.39-1.87.amzn1
httpd24-debuginfo-2.4.39-1.87.amzn1
mod24_session-2.4.39-1.87.amzn1
httpd24-tools-2.4.39-1.87.amzn1

noarch
httpd24-manual-2.4.39-1.87.amzn1

x86_64
mod24_session-2.4.39-1.87.amzn1
mod24_md-2.4.39-1.87.amzn1
mod24_ssl-2.4.39-1.87.amzn1
httpd24-2.4.39-1.87.amzn1
httpd24-devel-2.4.39-1.87.amzn1
mod24_ldap-2.4.39-1.87.amzn1
httpd24-debuginfo-2.4.39-1.87.amzn1
httpd24-tools-2.4.39-1.87.amzn1
mod24_proxy_html-2.4.39-1.87.amzn1

186639 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3935-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-5325, CVE-2014-9645, CVE-2015-9261, CVE-2016-2147, CVE-2016-2148, CVE-2017-15873, CVE-2017-16544, CVE-2018-1000517, CVE-2018-20679, CVE-2019-5747

Description

The scan detected that the host is missing the following update:
USN-3935-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004835.html

Ubuntu 16.04

busybox-initramfs_1.22.0-15ubuntu1.4
busybox_1.22.0-15ubuntu1.4
udhcpd_1.22.0-15ubuntu1.4
udhcpc_1.22.0-15ubuntu1.4
busybox-static_1.22.0-15ubuntu1.4

Ubuntu 18.10

udhcpc_1.27.2-2ubuntu4.1
busybox_1.27.2-2ubuntu4.1
busybox-static_1.27.2-2ubuntu4.1
udhcpd_1.27.2-2ubuntu4.1
busybox-initramfs_1.27.2-2ubuntu4.1

Ubuntu 14.04

busybox-static_1.21.0-1ubuntu1.4
busybox-initramfs_1.21.0-1ubuntu1.4
udhcpc_1.21.0-1ubuntu1.4
udhcpd_1.21.0-1ubuntu1.4
busybox_1.21.0-1ubuntu1.4

Ubuntu 18.04

busybox_1.27.2-2ubuntu3.2
busybox-static_1.27.2-2ubuntu3.2
udhcpc_1.27.2-2ubuntu3.2
busybox-initramfs_1.27.2-2ubuntu3.2
udhcpd_1.27.2-2ubuntu3.2

195003 - Fedora Linux 28 FEDORA-2019-13ba3be562 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18267, CVE-2018-13988, CVE-2018-20662, CVE-2019-9200, CVE-2019-9631

Description

The scan detected that the host is missing the following update:
FEDORA-2019-13ba3be562

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

poppler-0.62.0-20.fc28

195022 - Fedora Linux 30 FEDORA-2019-14040bfa27 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20662, CVE-2019-9200, CVE-2019-9631, CVE-2019-9903

Description

The scan detected that the host is missing the following update:
FEDORA-2019-14040bfa27

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 30

poppler-0.73.0-8.fc30

195028 - Fedora Linux 28 FEDORA-2019-b2d986c3e9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000852, CVE-2018-8786

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b2d986c3e9

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

freerdp-2.0.0-49.20190304git435872b.fc28
pidgin-sipe-1.24.0-3.fc28
gnome-boxes-3.28.5-2.fc28
remmina-1.3.3-1.fc28

195029 - Fedora Linux 28 FEDORA-2019-694e3aa4e8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12327, CVE-2018-7170, CVE-2019-8936

Description

The scan detected that the host is missing the following update:
FEDORA-2019-694e3aa4e8

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 28

ntp-4.2.8p13-1.fc28

195032 - Fedora Linux 29 FEDORA-2019-d04944813d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20662, CVE-2019-9200, CVE-2019-9631

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d04944813d

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

poppler-0.67.0-16.fc29

195034 - Fedora Linux 29 FEDORA-2019-be9add5b77 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16862, CVE-2018-16880, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-be9add5b77

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 29

kernel-tools-5.0.6-200.fc29
kernel-headers-5.0.6-200.fc29
kernel-5.0.6-200.fc29

196288 - Red Hat Enterprise Linux RHSA-2019-0708 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5787, CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5802, CVE-2019-5803

Description

The scan detected that the host is missing the following update:
RHSA-2019-0708

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00002.html

RHEL6D
i386
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

i686
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

x86_64
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

RHEL6S
i386
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

i686
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

x86_64
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

RHEL6WS
i386
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

i686
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

x86_64
chromium-browser-debuginfo-73.0.3683.75-1.el6_10
chromium-browser-73.0.3683.75-1.el6_10

24934 - (MSPT-Apr2019) Microsoft SharePoint Cross-Site-Scripting Vulnerability (CVE-2019-0831)

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

Risk Level: Medium

CVE: CVE-2019-0831

Description

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

Observation

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

The flaw is due to improper handling of a specially crafted web request. Successful exploitation could allow an authenticated attacker to perform cross-site scripting attacks.

24936 - (MSPT-Apr2019) Microsoft Windows Admin Center Privilege Escalation (CVE-2019-0813)

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

Risk Level: Medium

CVE: CVE-2019-0813

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 windows admin center. Successful exploitation could allow an authenticated user to gain elevated privileges.

24943 - (MSPT-Apr2019) Microsoft Edge Chakra Scripting Engine Remote Code Execution (CVE-2019-0829)

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

Risk Level: Medium

CVE: CVE-2019-0829

Description

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

Observation

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

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

24995 - (MSPT-Apr2019) Microsoft Windows LUAFV driver Privilege Escalation (CVE-2019-0836)

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

Risk Level: Medium

CVE: CVE-2019-0836

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 luafv 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.

25002 - (MSPT-Apr2019) Microsoft Team Foundation Server Cross-Site Scripting (CVE-2019-0866)

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

Risk Level: Medium

CVE: CVE-2019-0866

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

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

25003 - (MSPT-Apr2019) Microsoft Team Foundation Server Cross-Site Scripting (CVE-2019-0867)

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

Risk Level: Medium

CVE: CVE-2019-0867

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

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

25004 - (MSPT-Apr2019) Microsoft Team Foundation Server Cross-Site Scripting (CVE-2019-0868)

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

Risk Level: Medium

CVE: CVE-2019-0868

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

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

25005 - (MSPT-Apr2019) Microsoft Team Foundation Server Cross-Site Scripting (CVE-2019-0870)

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

Risk Level: Medium

CVE: CVE-2019-0870

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

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

25006 - (MSPT-Apr2019) Microsoft Team Foundation Server Cross-Site Scripting (CVE-2019-0871)

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

Risk Level: Medium

CVE: CVE-2019-0871

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to spoofing.

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

131331 - Debian Linux 9.0 DSA-4424-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3871

Description

The scan detected that the host is missing the following update:
DSA-4424-1

Observation

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

http://www.debian.org/security/2019/dsa-4424

Debian 9.0
all
pdns-server_4.0.3-1+deb9u4
pdns-backend-tinydns_4.0.3-1+deb9u4
pdns-tools_4.0.3-1+deb9u4
pdns-backend-pgsql_4.0.3-1+deb9u4
pdns-backend-opendbx_4.0.3-1+deb9u4
pdns-backend-remote_4.0.3-1+deb9u4
pdns-backend-mysql_4.0.3-1+deb9u4
pdns-backend-lua_4.0.3-1+deb9u4
pdns-backend-geoip_4.0.3-1+deb9u4
pdns-backend-ldap_4.0.3-1+deb9u4
pdns-backend-pipe_4.0.3-1+deb9u4
pdns-backend-odbc_4.0.3-1+deb9u4
pdns-backend-sqlite3_4.0.3-1+deb9u4
pdns-backend-mydns_4.0.3-1+deb9u4
pdns-backend-bind_4.0.3-1+deb9u4

147793 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:1128-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3871

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1128-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00041.html
https://lists.opensuse.org/opensuse-updates/2019-04/msg00046.html

SuSE Linux 15.0
x86_64
pdns-backend-sqlite3-4.1.2-lp150.3.10.1
pdns-backend-mysql-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-lua-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-ldap-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-lua-4.1.2-lp150.3.10.1
pdns-backend-sqlite3-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-remote-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-geoip-4.1.2-lp150.3.10.1
pdns-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-ldap-4.1.2-lp150.3.10.1
pdns-debugsource-4.1.2-lp150.3.10.1
pdns-backend-geoip-debuginfo-4.1.2-lp150.3.10.1
pdns-4.1.2-lp150.3.10.1
pdns-backend-mydns-4.1.2-lp150.3.10.1
pdns-backend-godbc-4.1.2-lp150.3.10.1
pdns-backend-mysql-4.1.2-lp150.3.10.1
pdns-backend-godbc-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-postgresql-4.1.2-lp150.3.10.1
pdns-backend-mydns-debuginfo-4.1.2-lp150.3.10.1
pdns-backend-remote-4.1.2-lp150.3.10.1
pdns-backend-postgresql-debuginfo-4.1.2-lp150.3.10.1

SuSE Linux 42.3
x86_64
pdns-4.0.3-18.1
pdns-backend-mysql-4.0.3-18.1
pdns-debuginfo-4.0.3-18.1
pdns-backend-postgresql-4.0.3-18.1
pdns-backend-sqlite3-debuginfo-4.0.3-18.1
pdns-backend-mydns-4.0.3-18.1
pdns-backend-ldap-debuginfo-4.0.3-18.1
pdns-backend-mydns-debuginfo-4.0.3-18.1
pdns-backend-geoip-4.0.3-18.1
pdns-backend-remote-debuginfo-4.0.3-18.1
pdns-backend-remote-4.0.3-18.1
pdns-backend-sqlite3-4.0.3-18.1
pdns-debugsource-4.0.3-18.1
pdns-backend-mysql-debuginfo-4.0.3-18.1
pdns-backend-geoip-debuginfo-4.0.3-18.1
pdns-backend-postgresql-debuginfo-4.0.3-18.1

pdns-backend-godbc-4.0.3-18.1
pdns-backend-godbc-debuginfo-4.0.3-18.1
pdns-backend-lua-debuginfo-4.0.3-18.1
pdns-backend-lua-4.0.3-18.1
pdns-backend-ldap-4.0.3-18.1

147797 - SuSE Linux 15.0 openSUSE-SU-2019:1159-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20346

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1159-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00078.html

SuSE Linux 15.0
i586
sqlite3-debugsource-3.27.2-lp150.2.3.1
sqlite3-devel-3.27.2-lp150.2.3.1
sqlite3-debuginfo-3.27.2-lp150.2.3.1
sqlite3-3.27.2-lp150.2.3.1
libsqlite3-0-3.27.2-lp150.2.3.1
libsqlite3-0-debuginfo-3.27.2-lp150.2.3.1

noarch
sqlite3-doc-3.27.2-lp150.2.3.1

x86_64
sqlite3-debugsource-3.27.2-lp150.2.3.1
sqlite3-devel-3.27.2-lp150.2.3.1
sqlite3-debuginfo-3.27.2-lp150.2.3.1
sqlite3-3.27.2-lp150.2.3.1
libsqlite3-0-32bit-3.27.2-lp150.2.3.1
libsqlite3-0-3.27.2-lp150.2.3.1
libsqlite3-0-debuginfo-3.27.2-lp150.2.3.1
libsqlite3-0-32bit-debuginfo-3.27.2-lp150.2.3.1

147798 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0852-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2018-18506, CVE-2019-5785, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9801, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0852-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005289.html

SuSE SLED 12 SP3
x86_64
MozillaFirefox-debugsource-60.6.1esr-109.63.2
MozillaFirefox-debuginfo-60.6.1esr-109.63.2
MozillaFirefox-translations-common-60.6.1esr-109.63.2
MozillaFirefox-60.6.1esr-109.63.2

SuSE SLED 12 SP4
x86_64
MozillaFirefox-debugsource-60.6.1esr-109.63.2
MozillaFirefox-debuginfo-60.6.1esr-109.63.2
MozillaFirefox-translations-common-60.6.1esr-109.63.2
MozillaFirefox-60.6.1esr-109.63.2

SuSE SLES 12 SP4
x86_64
MozillaFirefox-debugsource-60.6.1esr-109.63.2
MozillaFirefox-debuginfo-60.6.1esr-109.63.2
MozillaFirefox-translations-common-60.6.1esr-109.63.2
MozillaFirefox-60.6.1esr-109.63.2

SuSE SLES 12 SP3
x86_64
MozillaFirefox-debugsource-60.6.1esr-109.63.2
MozillaFirefox-debuginfo-60.6.1esr-109.63.2
MozillaFirefox-translations-common-60.6.1esr-109.63.2
MozillaFirefox-60.6.1esr-109.63.2

147800 - SuSE SLED 15 SUSE-SU-2019:0853-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2018-18506, CVE-2018-18509, CVE-2019-5785, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9801, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0853-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005290.html

SuSE SLED 15
x86_64
MozillaThunderbird-debugsource-60.6.1-3.28.1
MozillaThunderbird-translations-other-60.6.1-3.28.1
MozillaThunderbird-60.6.1-3.28.1
MozillaThunderbird-debuginfo-60.6.1-3.28.1

MozillaThunderbird-translations-common-60.6.1-3.28.1

147801 - SuSE Linux 15.0 openSUSE-SU-2019:1176-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19416, CVE-2018-19517

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1176-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00086.html

SuSE Linux 15.0
x86_64
sysstat-debuginfo-12.0.2-lp150.7.1
sysstat-12.0.2-lp150.7.1
sysstat-debugsource-12.0.2-lp150.7.1
sysstat-isag-12.0.2-lp150.7.1

147803 - SuSE Linux 15.0 openSUSE-SU-2019:1141-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16412, CVE-2018-18544, CVE-2018-20467, CVE-2019-7175, CVE-2019-7395, CVE-2019-7396, CVE-2019-7397, CVE-2019-7398

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1141-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00067.html

SuSE Linux 15.0
i586
libMagickWand-7_Q16HDRI6-7.0.7.34-lp150.2.26.1
perl-PerlMagick-7.0.7.34-lp150.2.26.1
ImageMagick-extra-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-extra-7.0.7.34-lp150.2.26.1
perl-PerlMagick-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-7.0.7.34-lp150.2.26.1
ImageMagick-devel-7.0.7.34-lp150.2.26.1
libMagickCore-7_Q16HDRI6-7.0.7.34-lp150.2.26.1
libMagickWand-7_Q16HDRI6-debuginfo-7.0.7.34-lp150.2.26.1
libMagickCore-7_Q16HDRI6-debuginfo-7.0.7.34-lp150.2.26.1
libMagick++-devel-7.0.7.34-lp150.2.26.1
libMagick++-7_Q16HDRI4-debuginfo-7.0.7.34-lp150.2.26.1

libMagick++-7_Q16HDRI4-7.0.7.34-lp150.2.26.1
ImageMagick-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-debugsource-7.0.7.34-lp150.2.26.1

noarch
ImageMagick-doc-7.0.7.34-lp150.2.26.1

x86_64
libMagickWand-7_Q16HDRI6-7.0.7.34-lp150.2.26.1
perl-PerlMagick-7.0.7.34-lp150.2.26.1
libMagickCore-7_Q16HDRI6-32bit-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-extra-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-extra-7.0.7.34-lp150.2.26.1
perl-PerlMagick-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-7.0.7.34-lp150.2.26.1
ImageMagick-devel-32bit-7.0.7.34-lp150.2.26.1
ImageMagick-devel-7.0.7.34-lp150.2.26.1
libMagick++-7_Q16HDRI4-32bit-7.0.7.34-lp150.2.26.1
libMagick++-devel-32bit-7.0.7.34-lp150.2.26.1
libMagick++-7_Q16HDRI4-32bit-debuginfo-7.0.7.34-lp150.2.26.1
libMagickCore-7_Q16HDRI6-7.0.7.34-lp150.2.26.1
libMagickCore-7_Q16HDRI6-32bit-7.0.7.34-lp150.2.26.1
libMagickWand-7_Q16HDRI6-debuginfo-7.0.7.34-lp150.2.26.1
libMagickCore-7_Q16HDRI6-debuginfo-7.0.7.34-lp150.2.26.1
libMagick++-devel-7.0.7.34-lp150.2.26.1
libMagick++-7_Q16HDRI4-debuginfo-7.0.7.34-lp150.2.26.1
libMagick++-7_Q16HDRI4-7.0.7.34-lp150.2.26.1
libMagickWand-7_Q16HDRI6-32bit-7.0.7.34-lp150.2.26.1
libMagickWand-7_Q16HDRI6-32bit-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-debuginfo-7.0.7.34-lp150.2.26.1
ImageMagick-debugsource-7.0.7.34-lp150.2.26.1

147809 - SuSE Linux 15.0 openSUSE-SU-2019:1161-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1161-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00079.html

SuSE Linux 15.0
x86_64
libtiff5-debuginfo-4.0.9-lp150.4.16.1
libtiff5-32bit-debuginfo-4.0.9-lp150.4.16.1
tiff-debuginfo-4.0.9-lp150.4.16.1
libtiff-devel-32bit-4.0.9-lp150.4.16.1
libtiff5-4.0.9-lp150.4.16.1
libtiff-devel-4.0.9-lp150.4.16.1
tiff-debugsource-4.0.9-lp150.4.16.1
tiff-4.0.9-lp150.4.16.1

libtiff5-32bit-4.0.9-lp150.4.16.1

i586
libtiff5-debuginfo-4.0.9-lp150.4.16.1
tiff-debuginfo-4.0.9-lp150.4.16.1
libtiff5-4.0.9-lp150.4.16.1
libtiff-devel-4.0.9-lp150.4.16.1
tiff-debugsource-4.0.9-lp150.4.16.1
tiff-4.0.9-lp150.4.16.1

147813 - SuSE SLES 12 SP3 SUSE-SU-2019:0901-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18249, CVE-2019-2024, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0901-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005309.html

SuSE SLES 12 SP3
x86_64
kernel-azure-base-debuginfo-4.4.176-4.25.1
kernel-azure-debugsource-4.4.176-4.25.1
kernel-azure-devel-4.4.176-4.25.1
kernel-azure-4.4.176-4.25.1
kernel-azure-base-4.4.176-4.25.1
kernel-azure-debuginfo-4.4.176-4.25.1
kernel-syms-azure-4.4.176-4.25.1

noarch
kernel-source-azure-4.4.176-4.25.1
kernel-devel-azure-4.4.176-4.25.1

147817 - SuSE Linux 15.0 openSUSE-SU-2019:1144-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20544, CVE-2018-20545, CVE-2018-20546, CVE-2018-20547, CVE-2018-20548, CVE-2018-20549

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1144-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00066.html

SuSE Linux 15.0
i586
caca-utils-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-plugins-0.99.beta19.git20171003-lp150.2.3.1
libcaca-ruby-0.99.beta19.git20171003-lp150.2.3.1
caca-utils-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca-devel-0.99.beta19.git20171003-lp150.2.3.1
libcaca-ruby-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca-debugsource-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-plugins-debuginfo-0.99.beta19.git20171003-lp150.2.3.1

noarch
python3-caca-0.99.beta19.git20171003-lp150.2.3.1

x86_64
libcaca-ruby-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
caca-utils-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-32bit-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-plugins-32bit-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-plugins-32bit-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca-debugsource-0.99.beta19.git20171003-lp150.2.3.1
caca-utils-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-32bit-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-plugins-0.99.beta19.git20171003-lp150.2.3.1
libcaca0-plugins-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca-ruby-debuginfo-0.99.beta19.git20171003-lp150.2.3.1
libcaca-devel-0.99.beta19.git20171003-lp150.2.3.1

147818 - SuSE Linux 15.0 openSUSE-SU-2019:1162-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2018-18506, CVE-2018-18509, CVE-2019-5785, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9801, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1162-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00083.html

SuSE Linux 15.0
x86_64
MozillaThunderbird-translations-common-60.6.1-lp150.3.37.1
MozillaThunderbird-buildsymbols-60.6.1-lp150.3.37.1
MozillaThunderbird-translations-other-60.6.1-lp150.3.37.1
MozillaThunderbird-debuginfo-60.6.1-lp150.3.37.1
MozillaThunderbird-debugsource-60.6.1-lp150.3.37.1

MozillaThunderbird-60.6.1-lp150.3.37.1

147821 - SuSE Linux 15.0 openSUSE-SU-2019:1164-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6486

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1164-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00082.html

SuSE Linux 15.0
x86_64
go1.11-1.11.5-lp150.6.4
go1.11-doc-1.11.5-lp150.6.4
go1.11-race-1.11.5-lp150.6.4

147824 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0899-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7572, CVE-2019-7573, CVE-2019-7574, CVE-2019-7575, CVE-2019-7576, CVE-2019-7577, CVE-2019-7578, CVE-2019-7635, CVE-2019-7636, CVE-2019-7637, CVE-2019-7638

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0899-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005311.html

SuSE SLED 12 SP3
x86_64
SDL-debugsource-1.2.15-15.11.1
libSDL-1_2-0-debuginfo-1.2.15-15.11.1
libSDL-1_2-0-1.2.15-15.11.1

SuSE SLED 12 SP4
x86_64
SDL-debugsource-1.2.15-15.11.1
libSDL-1_2-0-debuginfo-1.2.15-15.11.1
libSDL-1_2-0-1.2.15-15.11.1

SuSE SLES 12 SP4
x86_64
SDL-debugsource-1.2.15-15.11.1

libSDL-1_2-0-debuginfo-1.2.15-15.11.1
libSDL-1_2-0-1.2.15-15.11.1
libSDL-1_2-0-32bit-1.2.15-15.11.1
libSDL-1_2-0-debuginfo-32bit-1.2.15-15.11.1

SuSE SLES 12 SP3
x86_64
SDL-debugsource-1.2.15-15.11.1
libSDL-1_2-0-debuginfo-1.2.15-15.11.1
libSDL-1_2-0-1.2.15-15.11.1
libSDL-1_2-0-32bit-1.2.15-15.11.1
libSDL-1_2-0-debuginfo-32bit-1.2.15-15.11.1

147827 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0913-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20346, CVE-2018-20506

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0913-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005313.html

SuSE SLED 12 SP3
x86_64
libsqlite3-0-debuginfo-3.8.10.2-9.3.1
libsqlite3-0-32bit-3.8.10.2-9.3.1
sqlite3-3.8.10.2-9.3.1
sqlite3-debuginfo-3.8.10.2-9.3.1
sqlite3-debugsource-3.8.10.2-9.3.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.3.1
libsqlite3-0-3.8.10.2-9.3.1

SuSE SLED 12 SP4
x86_64
libsqlite3-0-debuginfo-3.8.10.2-9.3.1
libsqlite3-0-32bit-3.8.10.2-9.3.1
sqlite3-3.8.10.2-9.3.1
sqlite3-debuginfo-3.8.10.2-9.3.1
sqlite3-debugsource-3.8.10.2-9.3.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.3.1
libsqlite3-0-3.8.10.2-9.3.1

SuSE SLES 12 SP4
x86_64
libsqlite3-0-debuginfo-3.8.10.2-9.3.1
libsqlite3-0-32bit-3.8.10.2-9.3.1
sqlite3-3.8.10.2-9.3.1
sqlite3-debuginfo-3.8.10.2-9.3.1
sqlite3-debugsource-3.8.10.2-9.3.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.3.1
libsqlite3-0-3.8.10.2-9.3.1

SuSE SLES 12 SP3
x86_64
libsqlite3-0-debuginfo-3.8.10.2-9.3.1
libsqlite3-0-32bit-3.8.10.2-9.3.1
sqlite3-3.8.10.2-9.3.1
sqlite3-debuginfo-3.8.10.2-9.3.1
sqlite3-debugsource-3.8.10.2-9.3.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-9.3.1
libsqlite3-0-3.8.10.2-9.3.1

163840 - Oracle Enterprise Linux ELSA-2019-4601 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10877, CVE-2018-10882

Description

The scan detected that the host is missing the following update:
ELSA-2019-4601

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008628.html

OEL6
x86_64
kernel-uek-doc-2.6.39-400.308.1.el6uek
kernel-uek-2.6.39-400.308.1.el6uek
kernel-uek-debug-devel-2.6.39-400.308.1.el6uek
kernel-uek-devel-2.6.39-400.308.1.el6uek
kernel-uek-firmware-2.6.39-400.308.1.el6uek
kernel-uek-debug-2.6.39-400.308.1.el6uek

i386
kernel-uek-doc-2.6.39-400.308.1.el6uek
kernel-uek-2.6.39-400.308.1.el6uek
kernel-uek-debug-devel-2.6.39-400.308.1.el6uek
kernel-uek-devel-2.6.39-400.308.1.el6uek
kernel-uek-firmware-2.6.39-400.308.1.el6uek
kernel-uek-debug-2.6.39-400.308.1.el6uek

182950 - FreeBSD clamav Multiple Vulnerabilities (84ce26c3-5769-11e9-abd6-001b217b3468)

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

Risk Level: Medium

CVE: CVE-2019-1785, CVE-2019-1786, CVE-2019-1787, CVE-2019-1788, CVE-2019-1789, CVE-2019-1798

Description

The scan detected that the host is missing the following update:
clamav -- multiple vulnerabilities (84ce26c3-5769-11e9-abd6-001b217b3468)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/84ce26c3-5769-11e9-abd6-001b217b3468.html

Affected packages:
clamav < 0.101.2,1

195013 - Fedora Linux 28 FEDORA-2019-c595a93536 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000877, CVE-2018-1000878, CVE-2018-1000879, CVE-2018-1000880, CVE-2019-1000019, CVE-2019-1000020

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c595a93536

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

libarchive-3.3.3-6.fc28

195026 - Fedora Linux 29 FEDORA-2019-817ff2201f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20230, CVE-2019-9211

Description

The scan detected that the host is missing the following update:
FEDORA-2019-817ff2201f

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

pspp-1.2.0-2.fc29

195030 - Fedora Linux 28 FEDORA-2019-9f28451404 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10194, CVE-2018-16802, CVE-2019-3835, CVE-2019-3838, CVE-2019-6116

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9f28451404

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

ghostscript-9.26-4.fc28

24937 - (MSPT-Apr2019) Microsoft Edge Improperly Handle Objects In Memory Information Disclosure (CVE-2019-0833)

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

Risk Level: Medium

CVE: CVE-2019-0833

Description

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

Observation

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

The flaw is due to improper handling of objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24939 - (MSPT-Apr2019) Microsoft Edge Chakra Scripting Engine Remote Code Execution (CVE-2019-0810)

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

Risk Level: Medium

CVE: CVE-2019-0810

Description

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

Observation

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

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

24944 - (MSPT-Apr2019) Microsoft Edge Chakra Scripting Engine Remote Code Execution (CVE-2019-0812)

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

Risk Level: Medium

CVE: CVE-2019-0812

Description

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

Observation

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

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

24947 - (MSPT-Apr2019) Microsoft Exchange Server OWA Spoofing (CVE-2019-0858)

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

Risk Level: Medium

CVE: CVE-2019-0858

Description

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

Observation

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

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

24948 - (MSPT-Apr2019) Microsoft Exchange Server OWA Spoofing (CVE-2019-0817)

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

Risk Level: Medium

CVE: CVE-2019-0817

Description

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

Observation

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

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

24960 - (MSPT-Apr2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0844)

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

Risk Level: Medium

CVE: CVE-2019-0844

Description

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

Observation

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

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

24965 - (MSPT-Apr2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0849)

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

Risk Level: Medium

CVE: CVE-2019-0849

Description

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

Observation

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

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

24967 - (MSPT-Apr2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0802)

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

Risk Level: Medium

CVE: CVE-2019-0802

Description

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

Observation

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

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

24970 - (MSPT-Apr2019) Microsoft Win32k Improperly Handle Objects in Memory Privilege Escalation (CVE-2019-0685)

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

Risk Level: Medium

CVE: CVE-2019-0685

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 due the 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.

24971 - (MSPT-Apr2019) Microsoft Windows Task Scheduler Information Disclosure (CVE-2019-0838)

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

Risk Level: Medium

CVE: CVE-2019-0838

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 task Scheduler 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.

24972 - (MSPT-Apr2019) Microsoft Windows LUAFV driver Privilege Escalation (CVE-2019-0730)

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

Risk Level: Medium

CVE: CVE-2019-0730

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 luafv 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.

24973 - (MSPT-Apr2019) Microsoft Windows LUAFV driver Privilege Escalation (CVE-2019-0731)

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

Risk Level: Medium

CVE: CVE-2019-0731

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 luafv 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.

24982 - (MSPT-Apr2019) Microsoft Scripting Engine Improperly Handle Objects In Memory Information Disclosure (CVE-2019-0835)

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

Risk Level: Medium

CVE: CVE-2019-0835

Description

A vulnerability in some versions of the Microsoft Scripting Engine could lead to information disclosure.

Observation

A vulnerability in some versions of the Microsoft Scripting Engine could lead to information disclosure.

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

24988 - (MSPT-Apr2019) Microsoft Device Guard UMCI Security Bypass (CVE-2019-0732)

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

Risk Level: Medium

CVE: CVE-2019-0732

Description

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

Observation

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

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

24989 - (MSPT-Apr2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0840)

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

Risk Level: Medium

CVE: CVE-2019-0840

Description

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

Observation

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

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

24991 - (MSPT-Apr2019) Microsoft Win32k Kernel Information Disclosure Vulnerability (CVE-2019-0814)

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

Risk Level: Medium

CVE: CVE-2019-0814

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 the win32k component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24992 - (MSPT-Apr2019) Microsoft Win32k Information Disclosure Vulnerability(CVE-2019-0848)

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

Risk Level: Medium

CVE: CVE-2019-0848

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 the win32k component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24993 - (MSPT-Apr2019) Microsoft Windows LUAFV driver Privilege Escalation (CVE-2019-0796)

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

Risk Level: Medium

CVE: CVE-2019-0796

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 luafv 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.

24994 - (MSPT-Apr2019) Microsoft Windows LUAFV driver Privilege Escalation (CVE-2019-0805)

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

Risk Level: Medium

CVE: CVE-2019-0805

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 luafv 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.

24996 - (MSPT-Apr2019) Microsoft Windows TCP/IP Stack Information Disclosure (CVE-2019-0688)

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

Risk Level: Medium

CVE: CVE-2019-0688

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 tcp/ip stack 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.

24997 - (MSPT-Apr2019) Microsoft DirectX Information Disclosure Vulnerability (CVE-2019-0837)

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

Risk Level: Medium

CVE: CVE-2019-0837

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

24998 - (MSPT-Apr2019) Microsoft Terminal Services Information Disclosure Vulnerability (CVE-2019-0839)

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

Risk Level: Medium

CVE: CVE-2019-0839

Description

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

Observation

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

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

24999 - (MSPT-Apr2019) Microsoft Windows Elevation Of Privilege Vulnerability (CVE-2019-0841)

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

Risk Level: Medium

CVE: CVE-2019-0841

Description

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

Observation

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

The flaw lies in the appx deployment 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.

25013 - (MSPT-Apr2019) Azure DevOps Server HTML Injection Vulnerability (CVE-2019-0869)

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

Risk Level: Medium

CVE: CVE-2019-0869

Description

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Azure DevOps Server could lead to spoofing.

The flaw lies in the Improperly Handles Web Requests component. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

25022 - (MSPT-Apr2019) Microsoft Azure DevOps Server 2019 Privilege Escalation (CVE-2019-0875)

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

Risk Level: Medium

CVE: CVE-2019-0875

Description

A vulnerability in some versions of Microsoft Azure DevOps Server 2019 could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Azure DevOps Server 2019 could lead to privilege escalation.

The flaw lies due to improper handling of project permissions. Successful exploitation could allow an attacker to gain elevated privileges. The exploit requires the attacker to have access to a project.

131330 - Debian Linux 9.0 DSA-4422-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0196, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
DSA-4422-1

Observation

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

http://www.debian.org/security/2019/dsa-4422

Debian 9.0
all
apache2_2.4.25-3+deb9u7

147795 - SuSE Linux 42.3 openSUSE-SU-2019:1173-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1559, CVE-2019-5737, CVE-2019-5739

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1173-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00089.html

SuSE Linux 42.3
i586
nodejs6-debuginfo-6.17.0-21.1
nodejs6-6.17.0-21.1
npm6-6.17.0-21.1
nodejs6-devel-6.17.0-21.1
nodejs6-debugsource-6.17.0-21.1

noarch
nodejs6-docs-6.17.0-21.1

x86_64
nodejs6-debuginfo-6.17.0-21.1
nodejs6-6.17.0-21.1
npm6-6.17.0-21.1
nodejs6-devel-6.17.0-21.1
nodejs6-debugsource-6.17.0-21.1

147810 - SuSE Linux 42.3 openSUSE-SU-2019:1142-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6196, CVE-2018-6197, CVE-2018-6198

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1142-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00059.html

SuSE Linux 42.3
x86_64
w3m-debuginfo-0.5.3.git20161120-164.3.1
w3m-inline-image-0.5.3.git20161120-164.3.1
w3m-debugsource-0.5.3.git20161120-164.3.1
w3m-inline-image-debuginfo-0.5.3.git20161120-164.3.1
w3m-0.5.3.git20161120-164.3.1

i586
w3m-debuginfo-0.5.3.git20161120-164.3.1
w3m-inline-image-0.5.3.git20161120-164.3.1
w3m-debugsource-0.5.3.git20161120-164.3.1
w3m-inline-image-debuginfo-0.5.3.git20161120-164.3.1
w3m-0.5.3.git20161120-164.3.1

147819 - SuSE Linux 15.0 openSUSE-SU-2019:1147-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1543

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1147-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00058.html

SuSE Linux 15.0
x86_64
libopenssl1_1-debuginfo-1.1.0i-lp150.3.22.3
openssl-1_1-debuginfo-1.1.0i-lp150.3.22.3
libopenssl-1_1-devel-1.1.0i-lp150.3.22.3
openssl-1_1-1.1.0i-lp150.3.22.3
libopenssl1_1-hmac-1.1.0i-lp150.3.22.3
libopenssl1_1-1.1.0i-lp150.3.22.3
openssl-1_1-debugsource-1.1.0i-lp150.3.22.3

noarch
openssl-1_1-doc-1.1.0i-lp150.3.22.3

178729 - Gentoo Linux GLSA-201904-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-10

Observation

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

https://security.gentoo.org/glsa/201904-10

Affected packages:
net-mail/mailman < 2.1.29

178730 - Gentoo Linux GLSA-201904-09 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-09

Observation

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

https://security.gentoo.org/glsa/201904-09

Affected packages:
app-emulation/xen < 4.10.3-r1
app-emulation/xen-pvgrub < 4.10.3
app-emulation/xen-tools < 4.10.3-r2

186651 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3937-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0196, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
USN-3937-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004836.html

Ubuntu 16.04

apache2-bin_2.4.18-2ubuntu3.10

Ubuntu 18.10

apache2-bin_2.4.34-1ubuntu2.1

Ubuntu 14.04

apache2-bin_2.4.7-1ubuntu4.22

Ubuntu 18.04

apache2-bin_2.4.29-1ubuntu4.6

195012 - Fedora Linux 28 FEDORA-2019-86f32cbab1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-86f32cbab1

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

python3-3.6.8-3.fc28

195016 - Fedora Linux 30 FEDORA-2019-fe6d1fbffa Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9578

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fe6d1fbffa

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

libu2f-host-1.1.8-1.fc30

195019 - Fedora Linux 28 FEDORA-2019-46df367eed Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16868, CVE-2019-3829, CVE-2019-3836

Description

The scan detected that the host is missing the following update:
FEDORA-2019-46df367eed

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

gnutls-3.6.5-3.fc28

195039 - Fedora Linux 30 FEDORA-2019-a6e1287e76 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10255, CVE-2019-9644

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a6e1287e76

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 30

python-notebook-5.7.8-1.fc30

196285 - Red Hat Enterprise Linux RHSA-2019-0711 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15473

Description

The scan detected that the host is missing the following update:
RHSA-2019-0711

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00004.html

RHEL6D
x86_64
openssh-ldap-5.3p1-124.el6_10

openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-debuginfo-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10

i386
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-debuginfo-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10

RHEL6S
i386
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-debuginfo-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10

x86_64
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-debuginfo-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10

RHEL6WS
x86_64
openssh-clients-5.3p1-124.el6_10
openssh-debuginfo-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10

i386
openssh-clients-5.3p1-124.el6_10
openssh-debuginfo-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10

196286 - Red Hat Enterprise Linux RHSA-2019-0710 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
RHSA-2019-0710

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00003.html

RHEL7D
x86_64
python-libs-2.7.5-77.el7_6
tkinter-2.7.5-77.el7_6
python-debuginfo-2.7.5-77.el7_6
python-test-2.7.5-77.el7_6
python-2.7.5-77.el7_6
python-debug-2.7.5-77.el7_6
python-tools-2.7.5-77.el7_6
python-devel-2.7.5-77.el7_6

RHEL7S
x86_64
python-libs-2.7.5-77.el7_6
tkinter-2.7.5-77.el7_6
python-debuginfo-2.7.5-77.el7_6
python-test-2.7.5-77.el7_6
python-2.7.5-77.el7_6
python-debug-2.7.5-77.el7_6
python-tools-2.7.5-77.el7_6
python-devel-2.7.5-77.el7_6

RHEL7WS
x86_64
python-libs-2.7.5-77.el7_6
tkinter-2.7.5-77.el7_6
python-debuginfo-2.7.5-77.el7_6
python-test-2.7.5-77.el7_6
python-2.7.5-77.el7_6
python-debug-2.7.5-77.el7_6
python-tools-2.7.5-77.el7_6
python-devel-2.7.5-77.el7_6

131325 - Debian Linux 9.0 DSA-4426-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10868

Description

The scan detected that the host is missing the following update:
DSA-4426-1

Observation

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

http://www.debian.org/security/2019/dsa-4426

Debian 9.0
all

tryton-server_4.2.1-2+deb9u1

147814 - SuSE Linux 15.0 openSUSE-SU-2019:1145-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19840, CVE-2018-19841

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1145-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00060.html

SuSE Linux 15.0
x86_64
libwavpack1-32bit-5.1.0-lp150.3.3.1
libwavpack1-5.1.0-lp150.3.3.1
libwavpack1-32bit-debuginfo-5.1.0-lp150.3.3.1
wavpack-devel-5.1.0-lp150.3.3.1
wavpack-debuginfo-5.1.0-lp150.3.3.1
libwavpack1-debuginfo-5.1.0-lp150.3.3.1
wavpack-debugsource-5.1.0-lp150.3.3.1
wavpack-5.1.0-lp150.3.3.1

i586
libwavpack1-5.1.0-lp150.3.3.1
wavpack-devel-5.1.0-lp150.3.3.1
wavpack-debuginfo-5.1.0-lp150.3.3.1
libwavpack1-debuginfo-5.1.0-lp150.3.3.1
wavpack-debugsource-5.1.0-lp150.3.3.1
wavpack-5.1.0-lp150.3.3.1

147815 - SuSE Linux 15.0 openSUSE-SU-2019:1163-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3824

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1163-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00071.html

SuSE Linux 15.0
x86_64
ldb-tools-1.2.3-lp150.7.2

python3-ldb-32bit-1.2.3-lp150.7.2
python3-ldb-debuginfo-1.2.3-lp150.7.2
libldb-devel-1.2.3-lp150.7.2
libldb1-debuginfo-1.2.3-lp150.7.2
ldb-debugsource-1.2.3-lp150.7.2
ldb-tools-debuginfo-1.2.3-lp150.7.2
python3-ldb-1.2.3-lp150.7.2
python-ldb-1.2.3-lp150.7.2
libldb1-32bit-debuginfo-1.2.3-lp150.7.2
python3-ldb-devel-1.2.3-lp150.7.2
python-ldb-32bit-1.2.3-lp150.7.2
python-ldb-32bit-debuginfo-1.2.3-lp150.7.2
python-ldb-debuginfo-1.2.3-lp150.7.2
libldb1-1.2.3-lp150.7.2
python-ldb-devel-1.2.3-lp150.7.2
libldb1-32bit-1.2.3-lp150.7.2
python3-ldb-32bit-debuginfo-1.2.3-lp150.7.2

i586
python3-ldb-debuginfo-1.2.3-lp150.7.2
libldb-devel-1.2.3-lp150.7.2
libldb1-debuginfo-1.2.3-lp150.7.2
ldb-tools-debuginfo-1.2.3-lp150.7.2
ldb-tools-1.2.3-lp150.7.2
python-ldb-devel-1.2.3-lp150.7.2
libldb1-1.2.3-lp150.7.2
python-ldb-debuginfo-1.2.3-lp150.7.2
python3-ldb-devel-1.2.3-lp150.7.2
python3-ldb-1.2.3-lp150.7.2
python-ldb-1.2.3-lp150.7.2
ldb-debugsource-1.2.3-lp150.7.2

147816 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0891-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6778, CVE-2019-9824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0891-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005305.html

SuSE SLED 12 SP4
x86_64
xen-libs-32bit-4.11.1_04-2.6.1
xen-libs-4.11.1_04-2.6.1
xen-debugsource-4.11.1_04-2.6.1
xen-libs-debuginfo-4.11.1_04-2.6.1
xen-4.11.1_04-2.6.1
xen-libs-debuginfo-32bit-4.11.1_04-2.6.1

SuSE SLES 12 SP4

x86_64
xen-tools-domU-4.11.1_04-2.6.1
xen-tools-domU-debuginfo-4.11.1_04-2.6.1
xen-libs-32bit-4.11.1_04-2.6.1
xen-doc-html-4.11.1_04-2.6.1
xen-tools-4.11.1_04-2.6.1
xen-tools-debuginfo-4.11.1_04-2.6.1
xen-libs-4.11.1_04-2.6.1
xen-debugsource-4.11.1_04-2.6.1
xen-libs-debuginfo-4.11.1_04-2.6.1
xen-4.11.1_04-2.6.1
xen-libs-debuginfo-32bit-4.11.1_04-2.6.1

147822 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:1166-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9917

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1166-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00077.html
https://lists.opensuse.org/opensuse-updates/2019-04/msg00074.html

SuSE Linux 15.0
x86_64
znc-perl-debuginfo-1.7.2-lp150.25.1
znc-tcl-debuginfo-1.7.2-lp150.25.1
znc-debugsource-1.7.2-lp150.25.1
znc-debuginfo-1.7.2-lp150.25.1
znc-python3-1.7.2-lp150.25.1
znc-python3-debuginfo-1.7.2-lp150.25.1
znc-devel-1.7.2-lp150.25.1
znc-perl-1.7.2-lp150.25.1
znc-1.7.2-lp150.25.1
znc-tcl-1.7.2-lp150.25.1

noarch
znc-perl-1.7.2-bp150.2.3.1
znc-debuginfo-1.7.2-bp150.2.3.1
znc-lang-1.7.2-lp150.25.1
znc-python3-1.7.2-bp150.2.3.1
znc-debugsource-1.7.2-bp150.2.3.1
znc-tcl-1.7.2-bp150.2.3.1
znc-1.7.2-bp150.2.3.1
znc-perl-debuginfo-1.7.2-bp150.2.3.1
znc-python3-debuginfo-1.7.2-bp150.2.3.1
znc-devel-1.7.2-bp150.2.3.1
znc-tcl-debuginfo-1.7.2-bp150.2.3.1

SuSE Linux 42.3
i586

znc-debugsource-1.7.2-25.1
znc-perl-debuginfo-1.7.2-25.1
znc-tcl-debuginfo-1.7.2-25.1
znc-debuginfo-1.7.2-25.1
znc-perl-1.7.2-25.1
znc-devel-1.7.2-25.1
znc-1.7.2-25.1
znc-python3-1.7.2-25.1
znc-tcl-1.7.2-25.1
znc-python3-debuginfo-1.7.2-25.1

noarch
znc-lang-1.7.2-25.1

x86_64
znc-debugsource-1.7.2-25.1
znc-perl-debuginfo-1.7.2-25.1
znc-tcl-debuginfo-1.7.2-25.1
znc-debuginfo-1.7.2-25.1
znc-perl-1.7.2-25.1
znc-devel-1.7.2-25.1
znc-1.7.2-25.1
znc-python3-1.7.2-25.1
znc-tcl-1.7.2-25.1
znc-python3-debuginfo-1.7.2-25.1

147823 - SuSE Linux 42.3 openSUSE-SU-2019:1175-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1559

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1175-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00090.html

SuSE Linux 42.3
i586
openssl-cavs-debuginfo-1.0.2j-35.1
libopenssl1_0_0-hmac-1.0.2j-35.1
libopenssl-devel-1.0.2j-35.1
libopenssl1_0_0-1.0.2j-35.1
openssl-debuginfo-1.0.2j-35.1
openssl-debugsource-1.0.2j-35.1
libopenssl1_0_0-debuginfo-1.0.2j-35.1
openssl-1.0.2j-35.1
openssl-cavs-1.0.2j-35.1

noarch
openssl-doc-1.0.2j-35.1

x86_64

openssl-cavs-debuginfo-1.0.2j-35.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-35.1
libopenssl1_0_0-debuginfo-1.0.2j-35.1
openssl-debugsource-1.0.2j-35.1
libopenssl-devel-1.0.2j-35.1
openssl-cavs-1.0.2j-35.1
openssl-1.0.2j-35.1
libopenssl1_0_0-32bit-1.0.2j-35.1
libopenssl1_0_0-hmac-32bit-1.0.2j-35.1
libopenssl1_0_0-hmac-1.0.2j-35.1
libopenssl-devel-32bit-1.0.2j-35.1
libopenssl1_0_0-1.0.2j-35.1
openssl-debuginfo-1.0.2j-35.1

171086 - Amazon Linux AMI ALAS-2019-1187 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5741

Description

The scan detected that the host is missing the following update:
ALAS-2019-1187

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1187.html

Amazon Linux AMI
x86_64
bind-libs-9.8.2-0.68.rc1.59.amzn1
bind-chroot-9.8.2-0.68.rc1.59.amzn1
bind-devel-9.8.2-0.68.rc1.59.amzn1
bind-utils-9.8.2-0.68.rc1.59.amzn1
bind-sdb-9.8.2-0.68.rc1.59.amzn1
bind-9.8.2-0.68.rc1.59.amzn1
bind-debuginfo-9.8.2-0.68.rc1.59.amzn1

i686
bind-libs-9.8.2-0.68.rc1.59.amzn1
bind-chroot-9.8.2-0.68.rc1.59.amzn1
bind-devel-9.8.2-0.68.rc1.59.amzn1
bind-utils-9.8.2-0.68.rc1.59.amzn1
bind-sdb-9.8.2-0.68.rc1.59.amzn1
bind-9.8.2-0.68.rc1.59.amzn1
bind-debuginfo-9.8.2-0.68.rc1.59.amzn1

171087 - Amazon Linux AMI ALAS-2019-1188 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5407, CVE-2019-1559

Description

The scan detected that the host is missing the following update:
ALAS-2019-1188

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1188.html

Amazon Linux AMI
x86_64
openssl-perl-1.0.2k-16.150.amzn1
openssl-1.0.2k-16.150.amzn1
openssl-devel-1.0.2k-16.150.amzn1
openssl-debuginfo-1.0.2k-16.150.amzn1
openssl-static-1.0.2k-16.150.amzn1

i686
openssl-perl-1.0.2k-16.150.amzn1
openssl-debuginfo-1.0.2k-16.150.amzn1
openssl-devel-1.0.2k-16.150.amzn1
openssl-static-1.0.2k-16.150.amzn1
openssl-1.0.2k-16.150.amzn1

186642 - Ubuntu Linux 14.04 USN-3942-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
USN-3942-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004844.html

Ubuntu 14.04

icedtea-7-jre-jamvm_7u211-2.6.17-0ubuntu0.1
openjdk-7-jdk_7u211-2.6.17-0ubuntu0.1
openjdk-7-jre_7u211-2.6.17-0ubuntu0.1

186649 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3934-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3934-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004834.html

Ubuntu 16.04

libpolkit-backend-1-0_0.105-14.1ubuntu0.5
policykit-1_0.105-14.1ubuntu0.5

Ubuntu 18.10

policykit-1_0.105-21ubuntu0.4
libpolkit-backend-1-0_0.105-21ubuntu0.4

Ubuntu 14.04

policykit-1_0.105-4ubuntu3.14.04.6
libpolkit-backend-1-0_0.105-4ubuntu3.14.04.6

Ubuntu 18.04

libpolkit-backend-1-0_0.105-20ubuntu0.18.04.5
policykit-1_0.105-20ubuntu0.18.04.5

195000 - Fedora Linux 30 FEDORA-2019-ea0f30909a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18409

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ea0f30909a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

tcpflow-1.5.0-4.fc30

195002 - Fedora Linux 30 FEDORA-2019-961cda41f0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3882, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-961cda41f0

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

kernel-tools-5.0.6-300.fc30
kernel-5.0.6-300.fc30
kernel-headers-5.0.6-300.fc30

195008 - Fedora Linux 28 FEDORA-2019-9f891cd83a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-0494, CVE-2018-20483, CVE-2019-5953

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9f891cd83a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 28

wget-1.20.3-1.fc28

195011 - Fedora Linux 28 FEDORA-2019-fd54b80806 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10906

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fd54b80806

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

fuse-2.9.9-1.fc28

195021 - Fedora Linux 30 FEDORA-2019-bce274cbf6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9844

Description

The scan detected that the host is missing the following update:
FEDORA-2019-bce274cbf6

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

nodejs-simple-markdown-0.4.4-1.fc30

196287 - Red Hat Enterprise Linux RHSA-2019-0717 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13405

Description

The scan detected that the host is missing the following update:
RHSA-2019-0717

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00005.html

RHEL6D
i386
python-perf-2.6.32-754.12.1.el6
kernel-debuginfo-common-i686-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-debuginfo-2.6.32-754.12.1.el6
python-perf-debuginfo-2.6.32-754.12.1.el6
perf-debuginfo-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
kernel-debuginfo-2.6.32-754.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-754.12.1.el6
kernel-firmware-2.6.32-754.12.1.el6
kernel-doc-2.6.32-754.12.1.el6

x86_64
kernel-2.6.32-754.12.1.el6

perf-debuginfo-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
kernel-debug-debuginfo-2.6.32-754.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-754.12.1.el6
python-perf-debuginfo-2.6.32-754.12.1.el6
kernel-debuginfo-common-i686-2.6.32-754.12.1.el6
kernel-debuginfo-2.6.32-754.12.1.el6
python-perf-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6

RHEL6S
i386
python-perf-2.6.32-754.12.1.el6
kernel-debuginfo-common-i686-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-debuginfo-2.6.32-754.12.1.el6
python-perf-debuginfo-2.6.32-754.12.1.el6
perf-debuginfo-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
kernel-debuginfo-2.6.32-754.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-754.12.1.el6
kernel-firmware-2.6.32-754.12.1.el6
kernel-doc-2.6.32-754.12.1.el6

x86_64
kernel-2.6.32-754.12.1.el6
perf-debuginfo-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
kernel-debug-debuginfo-2.6.32-754.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-754.12.1.el6
python-perf-debuginfo-2.6.32-754.12.1.el6
kernel-debuginfo-common-i686-2.6.32-754.12.1.el6
kernel-debuginfo-2.6.32-754.12.1.el6
python-perf-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6

RHEL6WS
i386
kernel-debuginfo-common-i686-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-debuginfo-2.6.32-754.12.1.el6
python-perf-debuginfo-2.6.32-754.12.1.el6
perf-debuginfo-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6

kernel-debuginfo-2.6.32-754.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-754.12.1.el6
kernel-firmware-2.6.32-754.12.1.el6
kernel-doc-2.6.32-754.12.1.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-debuginfo-2.6.32-754.12.1.el6
python-perf-debuginfo-2.6.32-754.12.1.el6
perf-debuginfo-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
kernel-debuginfo-2.6.32-754.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-754.12.1.el6

89016 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-096-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0211

Description

The scan detected that the host is missing the following update:
SSA:2019-096-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.450188

Slackware 14.0
x86_64
httpd-2.4.39-x86_64-1

Slackware 14.2
x86_64
httpd-2.4.39-x86_64-1

i586
httpd-2.4.39-i586-1

Slackware 14.1
x86_64
httpd-2.4.39-x86_64-1

89017 - Slackware Linux 14.2 SSA:2019-095-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
SSA:2019-095-02

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.342076

Slackware 14.2
x86_64
wget-1.20.3-x86_64-1

i586
wget-1.20.3-i586-1

89018 - Slackware Linux 14.2 SSA:2019-095-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2019-095-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.332670

Slackware 14.2
x86_64
openjpeg-2.3.1-x86_64-1

i586
openjpeg-2.3.1-i586-1

131326 - Debian Linux 9.0 DSA-4428-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3842

Description

The scan detected that the host is missing the following update:
DSA-4428-1

Observation

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

http://www.debian.org/security/2019/dsa-4428

Debian 9.0
all
systemd_232-25+deb9u11

131328 - Debian Linux 9.0 DSA-4425-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
DSA-4425-1

Observation

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

http://www.debian.org/security/2019/dsa-4425

Debian 9.0
all
wget_1.18-5+deb9u3

131329 - Debian Linux 9.0 DSA-4427-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3880

Description

The scan detected that the host is missing the following update:
DSA-4427-1

Observation

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

http://www.debian.org/security/2019/dsa-4427

Debian 9.0
all
samba_2:4.5.16+dfsg-1+deb9u1

147812 - SuSE Linux 42.3 openSUSE-SU-2019:1139-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12181

Description

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

openSUSE-SU-2019:1139-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00062.html

SuSE Linux 42.3
i586
ovmf-2017+git1492060560.b6d11d7c46-19.1
ovmf-tools-2017+git1492060560.b6d11d7c46-19.1

noarch
qemu-ovmf-ia32-2017+git1492060560.b6d11d7c46-19.1
qemu-ovmf-x86_64-2017+git1492060560.b6d11d7c46-19.1

x86_64
ovmf-2017+git1492060560.b6d11d7c46-19.1
ovmf-tools-2017+git1492060560.b6d11d7c46-19.1
qemu-ovmf-x86_64-debug-2017+git1492060560.b6d11d7c46-19.1

186644 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3940-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-1787, CVE-2019-1788, CVE-2019-1789

Description

The scan detected that the host is missing the following update:
USN-3940-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004838.html

Ubuntu 16.04

clamav_0.100.3+dfsg-0ubuntu0.16.04.1

Ubuntu 18.10

clamav_0.100.3+dfsg-0ubuntu0.18.10.1

Ubuntu 14.04

clamav_0.100.3+dfsg-0ubuntu0.14.04.1

Ubuntu 18.04

clamav_0.100.3+dfsg-0ubuntu0.18.04.1

186645 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3939-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3880

Description

The scan detected that the host is missing the following update:
USN-3939-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004839.html

Ubuntu 16.04

samba_4.3.11+dfsg-0ubuntu0.16.04.19
libsmbclient_4.3.11+dfsg-0ubuntu0.16.04.19

Ubuntu 18.10

libsmbclient_4.8.4+dfsg-2ubuntu2.3
samba_4.8.4+dfsg-2ubuntu2.3

Ubuntu 14.04

libsmbclient_4.3.11+dfsg-0ubuntu0.14.04.20
samba_4.3.11+dfsg-0ubuntu0.14.04.20

Ubuntu 18.04

samba_4.7.6+dfsg~ubuntu-0ubuntu2.9
libsmbclient_4.7.6+dfsg~ubuntu-0ubuntu2.9

195004 - Fedora Linux 30 FEDORA-2019-6194273461 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6194273461

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 30

thunderbird-60.6.1-1.fc30

195005 - Fedora Linux 29 FEDORA-2019-117e425677 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-117e425677

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 29

golang-googlecode-go-crypto-0-0.28.20190324gitb7391e9.fc29

195006 - Fedora Linux 29 FEDORA-2019-3a2cc6a0b9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3890

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3a2cc6a0b9

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

evolution-ews-3.30.5-2.fc29
evolution-data-server-3.30.5-2.fc29

195007 - Fedora Linux 30 FEDORA-2019-9effd63191 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0804

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9effd63191

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

WALinuxAgent-2.2.38-1.fc30

195009 - Fedora Linux 28 FEDORA-2019-a51d6c2384 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a51d6c2384

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

firefox-66.0.2-1.fc28

195010 - Fedora Linux 30 FEDORA-2019-1d78e14cfd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1d78e14cfd

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 30

php-7.3.4-1.fc30

195015 - Fedora Linux 29 FEDORA-2019-119b14075a Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-119b14075a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

httpd-2.4.39-2.fc29

195018 - Fedora Linux 28 FEDORA-2019-2903a24dce Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2903a24dce

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 28

clamav-0.101.2-1.fc28

195020 - Fedora Linux 30 FEDORA-2019-cf7695b470 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
FEDORA-2019-cf7695b470

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 30

httpd-2.4.39-2.fc30

195023 - Fedora Linux 28 FEDORA-2019-c1e6c6edd9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c1e6c6edd9

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

ntfs-3g-2017.3.23-11.fc28

195024 - Fedora Linux 29 FEDORA-2019-e396eacd61 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e396eacd61

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 29

ntfs-3g-2017.3.23-11.fc29

195025 - Fedora Linux 30 FEDORA-2019-b0c7f0d94a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b0c7f0d94a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 30

ntp-4.2.8p13-1.fc30

195031 - Fedora Linux 30 FEDORA-2019-fc4bac128f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fc4bac128f

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

pcsc-lite-1.8.25-1.fc30

195033 - Fedora Linux 29 FEDORA-2019-fa59f1ed49 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fa59f1ed49

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

clamav-0.101.2-1.fc29

195035 - Fedora Linux 28 FEDORA-2019-3f561ba0be Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3f561ba0be

Observation

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

For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=3

Fedora Core 28

golang-googlecode-go-crypto-0-0.25.20190324gitb7391e9.fc28

195036 - Fedora Linux 29 FEDORA-2019-f781d5c4c6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f781d5c4c6

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

ntp-4.2.8p13-1.fc29

195037 - Fedora Linux 30 FEDORA-2019-66142859a3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
FEDORA-2019-66142859a3

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 30

wget-1.20.3-1.fc30

195038 - Fedora Linux 29 FEDORA-2019-a66789a334 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a66789a334

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=2

Fedora Core 29

glpi-9.3.3-2.fc29

147806 - SuSE Linux 42.3 openSUSE-SU-2019:1174-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3811

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1174-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00088.html

SuSE Linux 42.3
x86_64
libipa_hbac-devel-1.13.4-15.1
python-ipa_hbac-debuginfo-1.13.4-15.1
sssd-ldap-1.13.4-15.1
python-sssd-config-1.13.4-15.1
sssd-debugsource-1.13.4-15.1
libipa_hbac0-1.13.4-15.1
libsss_nss_idmap0-debuginfo-1.13.4-15.1
libsss_nss_idmap-devel-1.13.4-15.1
python-sss_nss_idmap-debuginfo-1.13.4-15.1
sssd-tools-1.13.4-15.1
sssd-ipa-debuginfo-1.13.4-15.1
sssd-ldap-debuginfo-1.13.4-15.1
libsss_idmap0-debuginfo-1.13.4-15.1
libsss_idmap0-1.13.4-15.1
sssd-1.13.4-15.1
sssd-ipa-1.13.4-15.1
libsss_nss_idmap0-1.13.4-15.1
sssd-krb5-debuginfo-1.13.4-15.1
python-sss_nss_idmap-1.13.4-15.1
sssd-proxy-1.13.4-15.1
libsss_idmap-devel-1.13.4-15.1
libsss_sudo-1.13.4-15.1
sssd-ad-1.13.4-15.1
sssd-ad-debuginfo-1.13.4-15.1
sssd-debuginfo-1.13.4-15.1

sssd-krb5-common-1.13.4-15.1
sssd-krb5-common-debuginfo-1.13.4-15.1
libsss_sudo-debuginfo-1.13.4-15.1
python-ipa_hbac-1.13.4-15.1
sssd-krb5-1.13.4-15.1
sssd-tools-debuginfo-1.13.4-15.1
sssd-32bit-1.13.4-15.1
sssd-proxy-debuginfo-1.13.4-15.1
sssd-debuginfo-32bit-1.13.4-15.1
libipa_hbac0-debuginfo-1.13.4-15.1
python-sssd-config-debuginfo-1.13.4-15.1

i586
libipa_hbac-devel-1.13.4-15.1
python-ipa_hbac-debuginfo-1.13.4-15.1
sssd-ldap-1.13.4-15.1
python-sssd-config-1.13.4-15.1
sssd-debugsource-1.13.4-15.1
libipa_hbac0-1.13.4-15.1
libsss_nss_idmap0-debuginfo-1.13.4-15.1
libsss_nss_idmap-devel-1.13.4-15.1
python-sss_nss_idmap-debuginfo-1.13.4-15.1
sssd-tools-1.13.4-15.1
sssd-ipa-debuginfo-1.13.4-15.1
sssd-ldap-debuginfo-1.13.4-15.1
libsss_idmap0-debuginfo-1.13.4-15.1
libsss_idmap0-1.13.4-15.1
sssd-1.13.4-15.1
sssd-ipa-1.13.4-15.1
libsss_nss_idmap0-1.13.4-15.1
sssd-krb5-debuginfo-1.13.4-15.1
python-sss_nss_idmap-1.13.4-15.1
sssd-proxy-1.13.4-15.1
libsss_idmap-devel-1.13.4-15.1
libsss_sudo-1.13.4-15.1
sssd-ad-1.13.4-15.1
sssd-ad-debuginfo-1.13.4-15.1
sssd-debuginfo-1.13.4-15.1
sssd-krb5-common-1.13.4-15.1
sssd-krb5-common-debuginfo-1.13.4-15.1
libsss_sudo-debuginfo-1.13.4-15.1
python-ipa_hbac-1.13.4-15.1
sssd-krb5-1.13.4-15.1
sssd-tools-debuginfo-1.13.4-15.1
sssd-proxy-debuginfo-1.13.4-15.1
libipa_hbac0-debuginfo-1.13.4-15.1
python-sssd-config-debuginfo-1.13.4-15.1

195027 - Fedora Linux 29 FEDORA-2019-7a0497cbc2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20483, CVE-2019-5953

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7a0497cbc2

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/4/?count=200&page=1

Fedora Core 29

wget-1.20.3-1.fc29

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.

24536 - (HT209341) Apple macOS Multiple Vulnerabilities Prior To 10.14.2

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-4303, CVE-2018-4427, CVE-2018-4431, CVE-2018-4434, CVE-2018-4435, CVE-2018-4447, CVE-2018-4449, CVE-2018-4450, CVE-2018-4460, CVE-2018-4461, CVE-2018-4462, CVE-2018-4463, CVE-2018-4465

Update Details

Risk is updated

24544 - (HT209340) Apple iOS Multiple Vulnerabilities Prior To 12.1.1

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2018-4303, CVE-2018-4429, CVE-2018-4430, CVE-2018-4431, CVE-2018-4435, CVE-2018-4436, CVE-2018-4437, CVE-2018-4438, CVE-2018-4439, CVE-2018-4440, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4445, CVE-2018-4446, CVE-2018-4447, CVE-2018-4460, CVE-2018-4461, CVE-2018-4464, CVE-2018-4465

Update Details

Risk is updated

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

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

Risk Level: High

CVE: CVE-2019-0617

Update Details

Risk is updated

193976 - Fedora Linux 27 FEDORA-2018-6227e1ff4c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10242, CVE-2018-10243, CVE-2018-10244

Update Details

Risk is updated

193986 - Fedora Linux 28 FEDORA-2018-747d000693 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10242, CVE-2018-10243, CVE-2018-10244

Update Details

Risk is updated

24339 - (HT209141) Apple iCloud Vulnerabilities Prior To 7.7

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

Risk Level: Medium

CVE: CVE-2018-4191, CVE-2018-4197, CVE-2018-4299, CVE-2018-4306, CVE-2018-4309, CVE-2018-4311, CVE-2018-4312, CVE-2018-4314, CVE-2018-4315, CVE-2018-4316, CVE-2018-4317, CVE-2018-4318, CVE-2018-4319, CVE-2018-4323, CVE-2018-4328, CVE-2018-4345, CVE-2018-4358, CVE-2018-4359, CVE-2018-4360, CVE-2018-4361

Update Details

Risk is updated

24414 - (HT209196) Apple Safari Vulnerabilities Prior To 12.0.1

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-4372, CVE-2018-4373, CVE-2018-4374, CVE-2018-4375, CVE-2018-4376, CVE-2018-4377, CVE-2018-4378, CVE-2018-4382, CVE-2018-4386, CVE-2018-4392, CVE-2018-4409, CVE-2018-4416

Update Details

Risk is updated

24420 - (HT209197) Apple iTunes Vulnerabilities Prior To 12.9.1

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

Risk Level: Medium

CVE: CVE-2018-4372, CVE-2018-4373, CVE-2018-4374, CVE-2018-4375, CVE-2018-4376, CVE-2018-4377, CVE-2018-4378, CVE-2018-4382, CVE-2018-4386, CVE-2018-4392, CVE-2018-4394, CVE-2018-4398, CVE-2018-4409, CVE-2018-4416

Update Details

Risk is updated

24431 - (HT209198) Apple iCloud Vulnerabilities Prior To 7.8

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

Risk Level: Medium

CVE: CVE-2018-4372, CVE-2018-4373, CVE-2018-4374, CVE-2018-4375, CVE-2018-4376, CVE-2018-4377, CVE-2018-4378, CVE-2018-4382, CVE-2018-4386, CVE-2018-4392, CVE-2018-4398, CVE-2018-4409, CVE-2018-4416

Update Details

Risk is updated

24539 - (HT209345) Apple iTunes Vulnerabilities Prior To 12.9.2

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

Risk Level: Medium

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4439, CVE-2018-4440, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464

Update Details

Risk is updated

24545 - (HT209346) Apple iCloud Vulnerabilities Prior To 7.9

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

Risk Level: Medium

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4439, CVE-2018-4440, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464

Update Details

Risk is updated

24546 - (HT209344) Apple Safari Vulnerabilities Prior To 12.0.2

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4439, CVE-2018-4440, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4445, CVE-2018-4464

Update Details

Risk is updated

147587 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0146-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464

Update Details

Risk is updated

147595 - SuSE Linux 42.3 openSUSE-SU-2019:0108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464

Update Details

Risk is updated

186485 - Ubuntu Linux 18.04, 18.10 USN-3828-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4345, CVE-2018-4372, CVE-2018-4386

Update Details
Risk is updated

186534 - Ubuntu Linux 18.04, 18.10 USN-3854-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4437

Update Details
Risk is updated

194621 - Fedora Linux 29 FEDORA-2018-1a8582a7ee Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4437

Update Details
Risk is updated

194626 - Fedora Linux 28 FEDORA-2018-e2e8a07a01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4437

Update Details
Risk is updated

24198 - (HT209109) Apple Safari Vulnerabilities Prior To 12

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4195, CVE-2018-4307, CVE-2018-4329

Update Details
Risk is updated

182871 - FreeBSD Gitlab Arbitrary File Read In Gitlab Project Import (70b774a8-05bc-11e9-87ad-001b217b3468)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-20229

Update Details

Risk is updated

182945 - FreeBSD Kubectl Potential Directory Traversal (6a0129bf-54ad-11e9-987c-1c39475b9f84)

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

Risk Level: Medium

CVE: CVE-2019-1002101

Update Details

Risk is updated

182949 - FreeBSD Jupyter notebook Open Redirect Vulnerability (fe7e322f-522d-11e9-98b5-216e512dad89)

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

Risk Level: Medium

CVE: CVE-2019-10255

Update Details

FASLScript is updated

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

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

Risk Level: Medium

CVE: CVE-2019-0821

Update Details

Risk is updated

189600 - Fedora Linux 22 FEDORA-2015-10235 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3603

Update Details

Risk is updated

189601 - Fedora Linux 21 FEDORA-2015-10175 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3603

Update Details

Risk is updated

194398 - Fedora Linux 29 FEDORA-2018-a1f37d2f08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4345

Update Details

Risk is updated

194509 - Fedora Linux 28 FEDORA-2018-509fc4a5c8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4345

Update Details

Risk is updated

24308 - (HT209162) Apple iOS Multiple Vulnerabilities Prior To 12.0.1

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Low

CVE: CVE-2018-4379, CVE-2018-4380

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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

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

Copyright 2019 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates