2017-DEC-12
FSL version 7.5.980

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

22858 - (MSPT-Dec2017) Microsoft Malware Protection Engine Remote Code Execution (CVE-2017-11940)

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

Risk Level: High

CVE: CVE-2017-11940

Description

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

Observation

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

The flaw exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

22805 - (MSPT-Dec2017) Microsoft Office Web Request Sanitization Privilege Escalation (CVE-2017-11936)

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

Risk Level: High

CVE: CVE-2017-11936

Description

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

Observation

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

The flaw lies in the Web Request Sanitization component.Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

22808 - (MSPT-Dec2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-11889)

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

Risk Level: High

CVE: CVE-2017-11889

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

22814 - (MSPT-Dec2017) Microsoft Exchange Web Access Spoofing Vulnerability (CVE-2017-11932)

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

Risk Level: High

CVE: CVE-2017-11932

Description

A spoofing vulnerability is present in some versions of Microsoft Exchange.

Observation

A spoofing vulnerability is present in some versions of Microsoft Exchange.

The flaw lies in the Microsoft Exchange Web Access 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.

22815 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11886)

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

Risk Level: High

CVE: CVE-2017-11886

Description

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

Observation

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

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

22817 - (MSPT-Dec2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-11930)

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

Risk Level: High

CVE: CVE-2017-11930

Description

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

Observation

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

The flaw lies in a memory corruption error. 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.

22818 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11901)

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

Risk Level: High

CVE: CVE-2017-11901

Description

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

Observation

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

The flaw is due to improper handling 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.

22819 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11903)

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

Risk Level: High

CVE: CVE-2017-11903

Description

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

Observation

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

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

22822 - (MSPT-Dec2017) Microsoft Windows Device Guard Security Bypass (CVE-2017-11899)

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

Risk Level: High

CVE: CVE-2017-11899

Description

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

Observation

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

The flaw lies in the Device Guard component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions.

22825 - (MSPT-Dec2017) Microsoft Windows RRAS Remote Code Execution (CVE-2017-11885)

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

Risk Level: High

CVE: CVE-2017-11885

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

22830 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2017-11909)

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

Risk Level: High

CVE: CVE-2017-11909

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 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.

22836 - (MSPT-Dec2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-11888)

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

Risk Level: High

CVE: CVE-2017-11888

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 a memory corruption error. 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.

22837 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11918)

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

Risk Level: High

CVE: CVE-2017-11918

Description

A remote code execution vulnerability is present in some versions of Microsoft Edge.

Observation

A remote code execution vulnerability is present in some versions of Microsoft Edge.

The flaw lies in how the Scripting Engine handles objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22839 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11914)

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

Risk Level: High

CVE: CVE-2017-11914

Description

A remote code execution vulnerability is present in some versions of Microsoft Edge.

Observation

A remote code execution vulnerability is present in some versions of Microsoft Edge.

The flaw lies in how the Scripting Engine handles objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22842 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11913)

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

Risk Level: High

CVE: CVE-2017-11913

Description

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

Observation

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

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

22843 - (MSPT-Dec2017) Microsoft Windows ITS Protocol Traffic Information Disclosure (CVE-2017-11927)

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

Risk Level: High

CVE: CVE-2017-11927

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 ITS Protocol trafffic 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.

22846 - (MSPT-Dec2017) Microsoft Browser Information Disclosure (CVE-2017-11919)

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

Risk Level: High

CVE: CVE-2017-11919

Description

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

Observation

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

The flaw lies in the Browser's scripting engine 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.

22807 - (MSPT-Dec2017) Microsoft Office Memory Handling Information Disclosure (CVE-2017-11934)

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

Risk Level: Medium

CVE: CVE-2017-11934

Description

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

Observation

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

The flaw lies in the Memory Handling 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.

22816 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Information Disclosure (CVE-2017-11887)

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

Risk Level: Medium

CVE: CVE-2017-11887

Description

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

Observation

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

The flaw lies in the Scripting Engine 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.

22820 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Information Disclosure (CVE-2017-11906)

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

Risk Level: Medium

CVE: CVE-2017-11906

Description

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

Observation

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

The flaw 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.

22821 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11890)

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

Risk Level: Medium

CVE: CVE-2017-11890

Description

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

Observation

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

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

22823 - (MSPT-Dec2017) Microsoft Internet Explorer Browser Remote Code Execution (CVE-2017-11895)

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

Risk Level: Medium

CVE: CVE-2017-11895

Description

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

Observation

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

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

22827 - (MSPT-Dec2017) Microsoft Office Memory Handling Information Disclosure (CVE-2017-11934)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-11934

Description

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

Observation

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

The flaw lies in the Memory Handling 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.

22831 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2017-11910)

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

Risk Level: Medium

CVE: CVE-2017-11910

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 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.

22833 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2017-11905)

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

Risk Level: Medium

CVE: CVE-2017-11905

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 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.

22834 - (MSPT-Dec2017) Microsoft Browser Scripting Engine Memory Corruption Vulnerability (CVE-2017-11912)

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

Risk Level: Medium

CVE: CVE-2017-11912

Description

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

Observation

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

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

22835 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2017-11911)

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

Risk Level: Medium

CVE: CVE-2017-11911

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 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.

22838 - (MSPT-Dec2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-11893)

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

Risk Level: Medium

CVE: CVE-2017-11893

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 a memory corruption error. 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.

22841 - (MSPT-Dec2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11908)

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

Risk Level: Medium

CVE: CVE-2017-11908

Description

A remote code execution vulnerability is present in some versions of Microsoft Edge.

Observation

A remote code execution vulnerability is present in some versions of Microsoft Edge.

The flaw lies in how the Scripting Engine handles objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22844 - (MSPT-Dec2017) Microsoft Browser Remote Code Execution (CVE-2017-11894)

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

Risk Level: Medium

CVE: CVE-2017-11894

Description

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

Observation

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

The flaw lies in the Browser's 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.

22845 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11907)

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

Risk Level: Medium

CVE: CVE-2017-11907

Description

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

Observation

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

The flaw lies in the Scripting Engine component in the browser. 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.

22859 - (APSB17-42) Vulnerability In Adobe Flash Player

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

Risk Level: Medium

CVE: CVE-2017-11305

Description

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

Observation

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

A vulnerability is present in some versions of Adobe Flash Player. The flaw is due to cookie management in some browsers. Deletion of cookies in some browsers could lead to the reset of all Flash Player preferences.

The update provided by Adobe bulletin APSB17-42 resolves the issue. The target system is missing this update.

22860 - (APSB17-42) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-11305

Description

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

Observation

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

A vulnerability is present in some versions of Adobe Flash Player. The flaw is due to cookie management in some browsers. Deletion of cookies in some browsers could lead to the reset of all Flash Player preferences.

The update provided by Adobe bulletin APSB17-42 resolves the issue. The target system is missing this update.

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.

21160 - Oracle WebLogic Server Critical Patch Update January 2017

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

Risk Level: High

CVE: CVE-2017-3248

Update Details

FASLScript is updated

22040 - Oracle WebLogic Server Critical Patch Update April 2017

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

Risk Level: High

CVE: CVE-2016-1181, CVE-2017-3506, CVE-2017-3531, CVE-2017-5638

Update Details

FASLScript is updated

22188 - Oracle WebLogic Server Critical Patch Update July 2017

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

Risk Level: High

CVE: CVE-2013-2027, CVE-2017-10063, CVE-2017-10123, CVE-2017-10137, CVE-2017-10147, CVE-2017-10148, CVE-2017-10178, CVE-2017-5638

Update Details

FASLScript is updated

20345 - Oracle WebLogic Server Critical Patch Update July 2016

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

Risk Level: High

CVE: CVE-2016-3445, CVE-2016-3499, CVE-2016-3510, CVE-2016-3586

Update Details

FASLScript is updated

20729 - Oracle WebLogic Server Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2015-7501, CVE-2016-3505, CVE-2016-5488, CVE-2016-5531, CVE-2016-5535, CVE-2016-5601

Update Details

FASLScript is updated

22832 - (MSPT-Dec2017) Microsoft Windows Malware Protection Engine Remote Code Execution (CVE-2017-11937)

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

Risk Level: High

CVE: CVE-2017-11937

Update Details

Recommendation is updated

19973 - Oracle WebLogic Server Critical Patch Update April 2016

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

Risk Level: High

CVE: CVE-2016-0638, CVE-2016-0675, CVE-2016-0688, CVE-2016-0696, CVE-2016-0700, CVE-2016-3416

Update Details

FASLScript is updated

22666 - Oracle WebLogic Server Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2017-10152, CVE-2017-10271, CVE-2017-10334, CVE-2017-10336, CVE-2017-10352

Update Details

FASLScript is updated

22794 - MacOS High Sierra Login As Root With No Password Vulnerability

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-13872

Update Details

Description is updated Observation is updated Recommendation is updated Risk is updated CVE is updated Documentation is updated

130962 - Debian Linux 9.0 DSA-4053-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16943, CVE-2017-16944

Update Details
Risk is updated

182532 - FreeBSD xrdp Local User Can Cause A Denial Of Service (a66f9be2-d519-11e7-9866-c85b763a2f96)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16927

Update Details
Risk is updated

185986 - Ubuntu Linux 17.04, 17.10 USN-3493-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16943

Update Details
Risk is updated

130942 - Debian Linux 8.0, 9.0 DSA-4039-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-16853

Update Details
Risk is updated

130944 - Debian Linux 8.0, 9.0 DSA-4038-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-16852

Update Details
Risk is updated

146130 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3215-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-16852

Update Details

Risk is updated

146060 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2976-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8614, CVE-2016-8628, CVE-2016-9587, CVE-2017-7481, CVE-2017-7550

Update Details

Risk is updated

182535 - FreeBSD exim Remote DoS Attack In BDAT Processing (75dd622c-d5fd-11e7-b9fe-c13eb7bcbf4f)

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

Risk Level: Medium

CVE: CVE-2017-16944

Update Details

Risk is updated

185995 - Ubuntu Linux 17.04, 17.10 USN-3499-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16944

Update Details

Risk is updated

192874 - Fedora Linux 27 FEDORA-2017-c2729c23b0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7550

Update Details

Risk is updated

192897 - Fedora Linux 25 FEDORA-2017-008017c9fe Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7550

Update Details

Risk is updated

192905 - Fedora Linux 26 FEDORA-2017-8bf1b0c692 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7550

Update Details
Risk is updated

130710 - Debian Linux 8.0 DSA-3792-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3157

Update Details
Risk is updated

160242 - CentOS 6 CESA-2017-0979 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3157

Update Details
Risk is updated

175161 - Scientific Linux Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1704-17275)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2017-3157

Update Details
Risk is updated

192852 - Fedora Linux 26 FEDORA-2017-9fbb35aeda Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12193

Update Details
Risk is updated

192864 - Fedora Linux 25 FEDORA-2017-38b37120a2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12193

Update Details
Risk is updated

192880 - Fedora Linux 27 FEDORA-2017-ef58cbde27 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12193

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.