2017-DEC-07
FSL version 7.5.979

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

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

Description

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

Observation

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

The flaw is due to improper scanning a specially crafted file. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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.

91966 - Oracle Enterprise Linux ELSA-2015-2522 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

Update Details

Risk is updated

91970 - Oracle Enterprise Linux ELSA-2015-2521 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

Update Details

Risk is updated

91986 - Oracle Enterprise Linux ELSA-2015-2671 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

130946 - Debian Linux 8.0, 9.0 DSA-4041-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16844

Update Details
Risk is updated

141020 - Red Hat Enterprise Linux RHSA-2015-2522 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

141022 - Red Hat Enterprise Linux RHSA-2015-2523 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

141023 - Red Hat Enterprise Linux RHSA-2015-2521 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

141046 - Red Hat Enterprise Linux RHSA-2015-2671 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

141779 - Red Hat Enterprise Linux RHSA-2017-3269 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16844

Update Details
Risk is updated

160006 - CentOS 6 CESA-2015-2521 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

160014 - CentOS 5 CESA-2015-2671 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

170607 - Amazon Linux AMI ALAS-2015-618 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

174795 - Scientific Linux Security ERRATA Important: apache-commons-collections on SL7.x (noarch) (1511-17483)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: High
CVE: CVE-2015-7501

Update Details
Risk is updated

174830 - Scientific Linux Security ERRATA Important: jakarta-commons-collections on SL6.x (noarch) (1511-17116)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: High
CVE: CVE-2015-7501

Update Details

Risk is updated

174835 - Scientific Linux Security ERRATA Important: jakarta-commons-collections on SL5.x i386/x86_64 (1512-3803)

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

Risk Level: High

CVE: CVE-2015-7501

Update Details

Risk is updated

182521 - FreeBSD procmail Heap-based Buffer Overflow (288f7cee-ced6-11e7-8ae9-0050569f0b83)

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

Risk Level: High

CVE: CVE-2017-16844

Update Details

Risk is updated

185972 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3483-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16844

Update Details

Risk is updated

22697 - Microsoft Office 2016 Click-To-Run November 2017 Updates

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

Risk Level: High

CVE: CVE-2017-11877, CVE-2017-11878, CVE-2017-11882, CVE-2017-11884

Update Details

Risk is updated

146100 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3096-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16667

Update Details

Risk is updated

192928 - Fedora Linux 25 FEDORA-2017-8016cc0bd0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16667

Update Details
Risk is updated

192962 - Fedora Linux 26 FEDORA-2017-ebee750022 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16667

Update Details
Risk is updated

192976 - Fedora Linux 27 FEDORA-2017-898a922aff Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16667

Update Details
Risk is updated

22781 - (VMSA-2017-0018) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2017-4934, CVE-2017-4938

Update Details
Risk is updated

192931 - Fedora Linux 26 FEDORA-2017-62e3a94f2a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-15115

Update Details
Risk is updated

192959 - Fedora Linux 27 FEDORA-2017-f73d3f1fc4 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-15115

Update Details
Risk is updated

192966 - Fedora Linux 25 FEDORA-2017-1b4d140781 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15115

Update Details

Risk is updated

22650 - Apache OpenOffice Multiple Vulnerabilities Prior To 4.1.4

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

Risk Level: Medium

CVE: CVE-2017-12607, CVE-2017-12608, CVE-2017-3157, CVE-2017-9806

Update Details

Risk is updated

22761 - (VMSA-2017-0018) VMware Horizon View Client Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4935, CVE-2017-4936, CVE-2017-4937

Update Details

Risk is updated

22775 - (VMSA-2017-0018) VMware Workstation Player Multiple Vulnerabilities II

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

Risk Level: Medium

CVE: CVE-2017-4935, CVE-2017-4936, CVE-2017-4937, CVE-2017-4939

Update Details

Risk is updated

96044 - Fedora Linux 27 FEDORA-2017-72b50be8d4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8807

Update Details

Risk is updated

96050 - Fedora Linux 26 FEDORA-2017-5525b6cb5a Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2017-8807

Update Details
Risk is updated

130912 - Debian Linux 9.0 DSA-4003-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000256

Update Details
Risk is updated

130938 - Debian Linux 8.0 DSA-4022-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12607, CVE-2017-12608

Update Details
Risk is updated

130947 - Debian Linux 9.0 DSA-4034-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-8807

Update Details
Risk is updated

145882 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0663-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4000

Update Details
Risk is updated

146021 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2850-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000256

Update Details
Risk is updated

146022 - SuSE Linux 42.3 openSUSE-SU-2017:2878-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000256

Update Details
Risk is updated

146042 - SuSE SLES 11 SP4 SUSE-SU-2017:2923-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15638

Update Details
Risk is updated

146044 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2932-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15638

Update Details
Risk is updated

146049 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2935-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15638

Update Details
Risk is updated

146051 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2940-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15638

Update Details
Risk is updated

170796 - Amazon Linux AMI ALAS-2017-817 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4000

Update Details

Risk is updated

182501 - FreeBSD Apache OpenOffice Multiple Vulnerabilities (27229c67-b8ff-11e7-9f79-ac9e174be3af)

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

Risk Level: Medium

CVE: CVE-2017-12607, CVE-2017-12608, CVE-2017-3157, CVE-2017-9806

Update Details

Risk is updated

185957 - Ubuntu Linux 14.04 USN-3472-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12607, CVE-2017-12608

Update Details

Risk is updated

185985 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3495-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000229

Update Details

Risk is updated

191779 - Fedora Linux 25 FEDORA-2017-8b0737b093 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4000

Update Details

Risk is updated

191837 - Fedora Linux 24 FEDORA-2017-a513be0939 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4000

Update Details

Risk is updated

192992 - Fedora Linux 25 FEDORA-2017-8575fbfe90 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2017-8807

Update Details
Risk is updated

22762 - Moxa NPort Device Multiple Vulnerabilities (ICSA-17-320-01)

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA
Risk Level: Medium
CVE: CVE-2017-14028, CVE-2017-16715, CVE-2017-16719

Update Details
Risk is updated

96040 - Fedora Linux 26 FEDORA-2017-1f52998c8b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15923

Update Details
Risk is updated

96051 - Fedora Linux 25 FEDORA-2017-f58bbbbdb0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15923

Update Details
Risk is updated

130936 - Debian Linux 8.0, 9.0 DSA-4033-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15923

Update Details
Risk is updated

145966 - SuSE SLES 12 SP2 SUSE-SU-2017:2601-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000198, CVE-2017-1000199

Update Details
Risk is updated

146098 - SuSE Linux 42.2 openSUSE-SU-2017:3097-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15923

Update Details
Risk is updated

146099 - SuSE Linux 42.3 openSUSE-SU-2017:3099-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15923

Update Details
Risk is updated

182165 - FreeBSD FreeBSD OpenSSL Remote DoS Vulnerability (0fcd3af0-a0fe-11e6-b1cf-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8610

Update Details
Risk is updated

182510 - FreeBSD konversation Crash In IRC Message Parsing (795ccee1-c7ed-11e7-ad7d-001e2a3f778d)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15923

Update Details
Risk is updated

182524 - FreeBSD frr BGP Mishandled Attribute Length On Error (bf266183-cec7-11e7-af2d-2047478f2f70)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15865

Update Details
Risk is updated

88895 - Slackware Linux 14.2 SSA:2017-306-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3736

Update Details

Risk is updated

130941 - Debian Linux 9.0 DSA-4030-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16651

Update Details

Risk is updated

130956 - Debian Linux 8.0, 9.0 DSA-4047-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15864, CVE-2017-16664

Update Details

Risk is updated

146086 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3090-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16837

Update Details

Risk is updated

146103 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3100-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16837

Update Details

Risk is updated

146107 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3054-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15864, CVE-2017-16664

Update Details

Risk is updated

182516 - FreeBSD roundcube File Disclosure Vulnerability (f622608c-c53c-11e7-a633-009c02a2ab30)

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

Risk Level: Medium
CVE: CVE-2017-16651

Update Details
Risk is updated

192916 - Fedora Linux 27 FEDORA-2017-cbc49efae8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-16651

Update Details
Risk is updated

192943 - Fedora Linux 26 FEDORA-2017-1560290881 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-16651

Update Details
Risk is updated

193007 - Fedora Linux 27 FEDORA-2017-612d3e009f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15110

Update Details
Risk is updated

193013 - Fedora Linux 25 FEDORA-2017-e40e02e0dd Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15110

Update Details
Risk is updated

193025 - Fedora Linux 26 FEDORA-2017-475529a26a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15110

Update Details
Risk 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.