

## MCAFFEE 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

#### 19945 - IBM AIX Openssl Multiple Vulnerabilities (openssl\_advisory18)

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800

#### Description

Multiple vulnerabilities are present in some versions of IBM AIX.

#### Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

#### 19949 - SMB Server Signing Not Enforced

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### Description

SMB service without signing enforced was detected on the host.

#### Observation

SMB/CIFS protocol provides shared access to files, printers on a network.

SMB service without signing enforced was detected on the host.

### 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.

#### 130453 - Debian Linux 8.0 DSA-3535-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2385

#### Update Details

Risk is updated

### 181893 - FreeBSD kmailio SEAS Module Heap Overflow (c428de09-ed69-11e5-92ce-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-2385

#### Update Details

Risk is updated

### 130460 - Debian Linux 7.0, 8.0 DSA-3543-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1235

#### Update Details

Risk is updated

### 19891 - PostgreSQL Multiple Vulnerabilities Prior To 9.5.2

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

Risk Level: High

CVE: CVE-2016-2193, CVE-2016-3065

#### Update Details

Risk is updated

### 181908 - FreeBSD PostgreSQL Minor Security Problems. (97a24d2e-f74c-11e5-8458-6cc21735f730)

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

Risk Level: High

CVE: CVE-2016-2193, CVE-2016-3065

#### Update Details

Risk is updated

### 19904 - (MS16-038) Cumulative Security Update for Microsoft Edge (3148532)

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

Risk Level: High

CVE: CVE-2016-0154, CVE-2016-0155, CVE-2016-0156, CVE-2016-0157, CVE-2016-0158, CVE-2016-0161

#### Update Details

Risk is updated

### 19922 - (MS16-045) Security Update for Windows Hyper-V (3143118)

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

Risk Level: High

CVE: CVE-2016-0088, CVE-2016-0089, CVE-2016-0090

[Update Details](#)

Risk is updated

### **19937 - (MS16-037) Cumulative Security Update for Internet Explorer (3148531)**

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

Risk Level: High

CVE: CVE-2016-0154, CVE-2016-0159, CVE-2016-0160, CVE-2016-0162, CVE-2016-0164, CVE-2016-0166

[Update Details](#)

Risk is updated

### **130442 - Debian Linux 7.0, 8.0 DSA-3518-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-3153, CVE-2016-3154

[Update Details](#)

Risk is updated

### **19887 - Apache Jetspeed Multiple Vulnerabilities Prior To 2.3.1**

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2016-0709, CVE-2016-0710, CVE-2016-0711, CVE-2016-0712, CVE-2016-2171

[Update Details](#)

Risk is updated

### **185199 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2919-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-1577, CVE-2016-2116

[Update Details](#)

Risk is updated

### **190449 - Fedora Linux 23 FEDORA-2016-372bb57df0 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-2392, CVE-2016-2538, CVE-2016-2841, CVE-2016-2857

[Update Details](#)

Risk is updated

## 190454 - Fedora Linux 24 FEDORA-2016-1b264ab4a4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2392, CVE-2016-2538, CVE-2016-2841, CVE-2016-2857

### Update Details

Risk is updated

## 190511 - Fedora Linux 22 FEDORA-2016-bfaf6a133b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2392, CVE-2016-2538, CVE-2016-2841, CVE-2016-2857

### 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.

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 2016 McAfee, Inc.  
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates