2017-FEB-10
FSL version 7.5.889

# 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

### 21200 - (K64292204) F5 BIG-IP OpenSSH Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-10010

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

Observation

F5's BIG-IP Products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the OpenSSH component. Successful exploitation could allow an attacker to escalate privileges.

### 21192 - IBM AIX Openssl SSL-Death-Alert Denial of Service Vulnerability (openssl_advisory22)

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

Risk Level: Medium

CVE: CVE-2016-8610

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaw is due to improper handling of ALERT packets during a SSL handshake. Successful exploitation could allow an attacker to cause denial of service condition.

### 21205 - (K32743437) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-7056

Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the OpenSSL Component. Successful exploitation could allow an attacker with local access to recover ECDSA P-256 private keys.

### 21213 - (K05121675) F5 BIG-IP TLS vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-9244

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the TLS session tickets management. Successful exploitation could allow a malicious user to obtain SSL session IDs from other sessions.

### 21201 - (K24324390) F5 BIG-IP OpenSSH Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-10011

Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the OpenSSL Component. Successful exploitation could allow an attacker to retrieve sensitive data.

## 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.

### 143861 - SuSE Linux 13.1 openSUSE-SU-2015:1240-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2180, CVE-2015-2181

Update Details

Risk is updated

### 130637 - Debian Linux 8.0 DSA-3724-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636

Update Details

Risk is updated

## 130638 - Debian Linux 8.0 DSA-3723-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636

Update Details

Risk is updated

## 130689 - Debian Linux 8.0 DSA-3775-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486

Update Details

Risk is updated

## 178355 - Gentoo Linux GLSA-201701-61 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9085

Update Details

Risk is updated

## 182274 - FreeBSD wordpress Multiple Vulnerabilities (14ea4458-e5cd-11e6-b56d-38d547003487)

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

Risk Level: High

CVE: CVE-2017-5610, CVE-2017-5611, CVE-2017-5612

Update Details

Risk is updated

## 190675 - Fedora Linux 24 FEDORA-2016-44821f9576 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4570, CVE-2016-4571

Update Details

Risk is updated

## 191330 - Fedora Linux 24 FEDORA-2016-160ec6525e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9085

Update Details

Risk is updated

## 191356 - Fedora Linux 24 FEDORA-2016-00d2f5c19f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9085

Update Details

Risk is updated

## 191379 - Fedora Linux 25 FEDORA-2016-26ef59f03d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9085

Update Details

Risk is updated

## 191395 - Fedora Linux 25 FEDORA-2016-301724f38e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9085

Update Details

Risk is updated

## 191435 - Fedora Linux 25 FEDORA-2016-c883d07fba Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636

Update Details

Risk is updated

## 21163 - Oracle VM VirtualBox Critical Patch Update January 2017

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

Risk Level: Medium

CVE: CVE-2016-5545, CVE-2017-3290, CVE-2017-3316, CVE-2017-3332

Update Details

Risk is updated

### 21164 - Oracle JRockit Critical Patch Update January 2017

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

Risk Level: Medium

CVE: CVE-2016-5546, CVE-2016-5547, CVE-2016-5552, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253

Update Details

Risk is updated

### 144809 - SuSE Linux 13.1 openSUSE-SU-2016:2127-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2181, CVE-2015-8864

Update Details

Risk is updated

### 144810 - SuSE Linux 13.2 openSUSE-SU-2016:2108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2181, CVE-2015-8864

Update Details

Risk is updated

### 20873 - (SOL06288381) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7977, CVE-2015-7978

Update Details

Risk is updated

### 21185 - (CTX220112) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-5300, CVE-2015-7704, CVE-2015-7705, CVE-2017-5572, CVE-2017-5573

Update Details

Risk is updated

### 37525 - IBM AIX IV84269 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details
Risk is updated

### 37526 - IBM AIX IV83984 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details
Risk is updated

### 37527 - IBM AIX IV83993 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details
Risk is updated

### 37528 - IBM AIX IV83994 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details
Risk is updated

### 37529 - IBM AIX IV83995 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details
Risk is updated

### 37530 - IBM AIX IV83992 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details

Risk is updated

### 37531 - IBM AIX IV83983 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Update Details

Risk is updated

### 96032 - Oracle Enterprise Linux ELSA-2016-0063 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

Risk is updated

### 130687 - Debian Linux 8.0 DSA-3774-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10165

Update Details

Risk is updated

### 132213 - Oracle VM OVMSA-2016-0006 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

Risk is updated

### 141069 - Red Hat Enterprise Linux RHSA-2016-0063 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

Risk is updated

### 160036 - CentOS 6, 7 CESA-2016-0063 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

Risk is updated

### 174892 - Scientific Linux Security ERRATA Important: ntp on SL6.x, SL7.x i386/x86_64 (1601-11088)

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

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

Risk is updated

### 191028 - Fedora Linux 25 FEDORA-2016-417ceefc85 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6264

Update Details

Risk is updated

### 191031 - Fedora Linux 24 FEDORA-2016-53cc023dd6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6264

Update Details

Risk is updated

### 145159 - SuSE Linux 13.2 openSUSE-SU-2017:0184-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8568, CVE-2016-8569

Update Details

Risk is updated

### 181901 - FreeBSD salt Insecure Configuration Of PAM External Authentication Service (6d25c306-f3bb-11e5-92ce-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-3176

Update Details

Risk is updated

### 182018 - FreeBSD tiff Buffer Overflow (c17fe91d-4aa6-11e6-a7bd-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-5102

Update Details
Risk is updated

### 182195 - FreeBSD ImageMagick7 Multiple Vulnerabilities (e1f67063-aab4-11e6-b2d3-60a44ce6887b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8862, CVE-2016-8866, CVE-2016-9298

Update Details
Risk is updated

### 182201 - FreeBSD ImageMagick Heap Overflow Vulnerability (19d35b0f-ba73-11e6-b1cf-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9298

Update Details
Risk is updated

### 191302 - Fedora Linux 23 FEDORA-2016-616a35205b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8568, CVE-2016-8569

Update Details
Risk is updated

### 191649 - Fedora Linux 25 FEDORA-2017-e6012e74b6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2583

Update Details
Risk is updated

### 191654 - Fedora Linux 24 FEDORA-2017-18ce368ba3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2583

Update Details

Risk is updated

### 181694 - FreeBSD Salt Information Disclosure (e6b974ab-9d35-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8034

Update Details

Risk is updated

### 182053 - FreeBSD FreeBSD Insecure Default Snmpd.config Permissions (7a31dfba-600a-11e6-a6c3-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-5677

Update Details

Risk is updated

### 190273 - Fedora Linux 22 FEDORA-2016-c1fd651bc0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8034

Update Details

Risk is updated

### 191602 - Fedora Linux 25 FEDORA-2017-e6a9108cce Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5026

Update Details

Risk is updated

### 191606 - Fedora Linux 24 FEDORA-2017-cdf8277947 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5026

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.