2016-JUL-04
FSL version 7.5.831

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

20247 - (SYM16-011) Symantec Endpoint Protection Manager Multiple Security Vulnerabilities

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3647, CVE-2016-3648, CVE-2016-3649, CVE-2016-3650, CVE-2016-3651, CVE-2016-3652, CVE-2016-3653, CVE-2016-5304, CVE-2016-5305, CVE-2016-5306, CVE-2016-5307

Description

Multiple vulnerabilities are present in some versions of Symantec Endpoint Protection Manager.

Observation

Symantec Endpoint Protection Manager enables the management of endpoint nodes of anti-malware for Windows, Mac and Linux computers.

Multiple vulnerabilities are present in some versions of Symantec Endpoint Protection Manager. The flaws lie in the SEPM Manager console. Successful exploitation could allow an attacker to bypass certain restrictions, obtain sensitive information, or perform remote code execution.

20239 - (VMSA-2016-0008) VMware vRealize Log Insight Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-2081, CVE-2016-2082

Description

Multiple vulnerabilities are present in some versions of VMware vRealize Log Insight.

Observation

VMware vRealize Log Insight delivers heterogeneous and scalable log management.

Multiple vulnerabilities are present in some versions of VMware vRealize Log Insight. The flaws lie in the web interface. Successful exploitation could allow an attacker to perform a web session hijacking or a content replacement without the user's authorization.

20242 - IBM WebSphere Application Server Liberty API Discovery Vulnerability (swg21984502)

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

Risk Level: Medium

CVE: CVE-2016-2945

Description

A privilege escalation vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile.

Observation

IBM WebSphere Application Server Liberty Profile is a Java EE application server.

A privilege escalation vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile. The flaw lies in the API Discovery feature. Successful exploitation could allow an authenticated attacker to escalate privileges.

20248 - (SYM16-011) Symantec Endpoint Protection Client Device Control Restriction Local Race Condition Bypass Vulnerability

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-8801

Description

A vulnerability is present in some versions of Symantec Endpoint Protection Client.

Observation

Symantec Endpoint Protection is an all-in-one antivirus software.

A vulnerability is present in some versions of Symantec Endpoint Protection Client. The flaw is due to a race condition in the device control. Successful exploitation could allow an attacker to bypass certain restriction.

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.

15824 - (SOL13233) F5 Traffic Management Microkernel Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-6016

Update Details

FASLScript is updated

14393 - Microsoft Internet Explorer Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

Observation is updated 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.