2018-JAN-15
FSL version 7.5.994

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

22955 - (VMSA-2017-0021) VMware vCenter Server Appliance Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4943

Description

A vulnerability is present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A vulnerability is present in some versions of VMware vCenter Server. The flaw lies in showlog plug-in component. Successful exploitation could allow an attacker to gain root level privileges on the target system.

22904 - (VMSA-2017-0021) VMware ESXi Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4933, CVE-2017-4940, CVE-2017-4941

Description

Multiple vulnerabilities are present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware ESXi. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code.

22905 - (VMSA-2017-0021) VMware ESXi Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4933, CVE-2017-4940, CVE-2017-4941

Description

Multiple vulnerabilities are present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware ESXi. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code.

22963 - IBM WebSphere Application Server Apache Commons Vulnerability (swg22011428)

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

Risk Level: High

CVE: CVE-2016-1000031

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in the Apache Commons FileUpload component. Successful exploitation could allow an attacker to execute arbitrary code.

22866 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.2

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

Risk Level: Medium

CVE: CVE-2017-7845

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw lies in the graphics processing component. Successful exploitation could allow an attacker to cause a denial of service condition.

22899 - Ecava IntegraXor SQL Injection Vulnerabilities Prior To 6.1.1215.0

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

Risk Level: Medium

CVE: CVE-2017-16733, CVE-2017-16735

Description

Multiple SQL injection vulnerabilities are present in some versions of Ecava IntegraXor.

Observation

Ecava IntegraXor is web-based HMI/SCADA software.

Multiple SQL injection vulnerabilities are present in some versions of Ecava IntegraXor. The flaws lie in how the product handles the validation of its input fields. Successful exploitation could allow an attacker to obtain sensitive information or generate an error in the database log on the affected system.

22902 - (SYM17-016) Symantec Messaging Gateway Directory Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-15532

Description

A vulnerability is present in some versions of Symantec Messaging Gateway.

Observation

Symantec Messaging Gateway is an email security solution.

A vulnerability is present in some versions of Symantec Messaging Gateway. The flaw is due to improper handling of user input. Successful exploitation could allow an attacker to access arbitrary files and directories.

22903 - (SYM17-016) Symantec Messaging Gateway Directory Traversal Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-15532

Description

A vulnerability is present in some versions of Symantec Messaging Gateway.

Observation

Symantec Messaging Gateway is an email security solution.

A vulnerability is present in some versions of Symantec Messaging Gateway. The flaw is due to improper handling of user input. Successful exploitation could allow an attacker to access arbitrary files and directories.

22956 - Siemens LOGO! Soft Comfort Unsecure Download Of Code Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-12740

Description

A vulnerability is present in some versions of Siemens LOGO! Soft Comfort.

Observation

Siemens LOGO! Soft Comfort is an engineering software to configure and program LOGO! controllers.

A vulnerability is present in some versions of Siemens LOGO! Soft Comfort. The flaw occurs due to false integrity verification of software packages. Successful exploitation could allow an attacker to bypass security restrictions.

22957 - (VMSA-2018-0002) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Pro.

Observation

VMware Workstation is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose sensitive information.

22958 - (CTX231390) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws are due to CPU speculative execution issues. Successful exploitation could allow malicious code running in a guest VM to access sensitive data from other VMs on the same host.

22971 - (VMSA-2018-0002) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow an attacker to disclose sensitive information.

22891 - Cisco Jabber Information Disclosure Vulnerability (cisco-sa-20171129-jabber2)

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

Risk Level: Low

CVE: CVE-2017-12361

Description

An information disclosure vulnerability is present in some versions of Cisco Jabber.

Observation

Cisco Jabber is Cisco unified communication software solution.

An information disclosure vulnerability is present in some versions of Cisco Jabber. The flaw lies in the random number generation for

file folders. Successful exploitation could allow an attacker to decrypt secure communications.

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.