2017-APR-21
FSL version 7.5.914

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

21573 - Skype Insecure Library Loading Vulnerability

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

Risk Level: High

CVE: CVE-2017-6517

Description

A DLL hijacking vulnerability is present in some versions of Microsoft Skype.

Observation

Microsoft Skype is a popular instant message and VoIP software.

A DLL hijacking vulnerability is present in some versions of Microsoft Skype. The flaw lies in skype.exe improperly loading a DLL. Successful exploitation could allow an attacker to execute arbitrary code.

21580 - NetIQ Privileged User Manager Prior To 2.4.1 HF2

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

Risk Level: High

CVE: CVE-2014-3569, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206, CVE-2015-0207, CVE-2015-0208, CVE-2015-0209, CVE-2015-0285, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0290, CVE-2015-0291, CVE-2015-0293, CVE-2015-1787, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, CVE-2015-1793, CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2015-3197, CVE-2016-0701, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-7052, CVE-2016-7055, CVE-2017-3731, CVE-2017-3732

Description

Multiple vulnerabilities are present in some versions of NetIQ Privileged User Manager.

Observation

NetIQ Privileged User Manager is a secure manager for elevated permission credentials.

Multiple vulnerabilities are present in some versions of NetIQ Privileged User Manager. The flaws lie in OpenSSL. Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, bypass security restrictions, cause a denial-of-service or have other unspecified impact via unknown vectors.

21631 - (HT207617) Apple iOS Multiple Vulnerabilities Prior To 10.3

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2016-3619, CVE-2016-9642, CVE-2016-9643, CVE-2017-2364, CVE-2017-2367, CVE-2017-2376, CVE-2017-2377, CVE-2017-2378, CVE-2017-2379, CVE-2017-2380, CVE-2017-2384, CVE-2017-2386, CVE-2017-2389, CVE-2017-2390, CVE-2017-2393, CVE-2017-2394, CVE-2017-2395, CVE-2017-2396, CVE-2017-2397, CVE-2017-2398, CVE-2017-2399, CVE-2017-2400, CVE-2017-2401, CVE-2017-2404, CVE-2017-2405, CVE-2017-2406, CVE-2017-2407, CVE-2017-2412, CVE-2017-2414, CVE-2017-2415, CVE-2017-2416, CVE-2017-2417, CVE-2017-2419, CVE-2017-2423, CVE-2017-2424, CVE-2017-2428, CVE-2017-2430, CVE-2017-2432, CVE-2017-2433, CVE-2017-2434, CVE-2017-2435, CVE-2017-2439, CVE-2017-2440, CVE-2017-2441, CVE-2017-2442, CVE-2017-2444, CVE-2017-2445, CVE-2017-2446, CVE-2017-2447, CVE-2017-2448, CVE-2017-2450, CVE-2017-2451, CVE-2017-2452, CVE-2017-2453, CVE-2017-2454, CVE-2017-2455, CVE-2017-2456, CVE-2017-2457, CVE-2017-2458, CVE-2017-2459, CVE-2017-2460, CVE-2017-2461, CVE-2017-2462, CVE-2017-2463, CVE-2017-2464, CVE-2017-2465, CVE-2017-2466, CVE-2017-2467, CVE-2017-2468, CVE-2017-2469, CVE-2017-2470, CVE-2017-2471, CVE-2017-2472, CVE-2017-2473, CVE-2017-2474, CVE-2017-2475, CVE-2017-2476, CVE-2017-2478, CVE-2017-2479, CVE-2017-2480, CVE-2017-2481, CVE-2017-2482, CVE-2017-2483, CVE-2017-2484, CVE-2017-2485, CVE-2017-2486, CVE-2017-2487, CVE-2017-2490, CVE-2017-5029

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

21572 - (HT207615) Apple macOS Multiple Vulnerabilities Prior To 10.12.4

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-0736, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-2161, CVE-2016-3619, CVE-2016-5387, CVE-2016-5636, CVE-2016-7056, CVE-2016-7585, 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-2016-8740, CVE-2016-8743, CVE-2016-9533, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9538, CVE-2016-9539, CVE-2016-9540, CVE-2016-9586, CVE-2016-9935, CVE-2017-2379, CVE-2017-2381, CVE-2017-2388, CVE-2017-2390, CVE-2017-2392, CVE-2017-2398, CVE-2017-2401, CVE-2017-2402, CVE-2017-2403, CVE-2017-2406, CVE-2017-2407, CVE-2017-2408, CVE-2017-2409, CVE-2017-2410, CVE-2017-2413, CVE-2017-2416, CVE-2017-2417, CVE-2017-2418, CVE-2017-2420, CVE-2017-2421, CVE-2017-2422, CVE-2017-2423, CVE-2017-2425, CVE-2017-2426, CVE-2017-2427, CVE-2017-2428, CVE-2017-2429, CVE-2017-2430, CVE-2017-2431, CVE-2017-2432, CVE-2017-2435, CVE-2017-2436, CVE-2017-2437, CVE-2017-2438, CVE-2017-2439, CVE-2017-2440, CVE-2017-2441, CVE-2017-2443, CVE-2017-2448, CVE-2017-2449, CVE-2017-2450, CVE-2017-2451, CVE-2017-2456, CVE-2017-2457, CVE-2017-2458, CVE-2017-2461, CVE-2017-2462, CVE-2017-2467, CVE-2017-2472, CVE-2017-2473, CVE-2017-2474, CVE-2017-2478, CVE-2017-2482, CVE-2017-2483, CVE-2017-2485, CVE-2017-2486, CVE-2017-2487, 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, CVE-2017-6974

Description

Multiple vulnerabilities are present in some versions of Apple macOS.

Observation

Apple macOS is the operating system developed by Apple.

Multiple vulnerabilities are present in some versions of Apple macOS. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, escalate privileges, retrieve sensitive data or remotely execute arbitrary code on the target system.

21577 - Google Chrome Multiple Vulnerabilities Prior To 57.0.2987.133

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive data, execute arbitrary code or affect availability.

21578 - Google Chrome Multiple Vulnerabilities Prior To 57.0.2987.133

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive data, execute arbitrary code or affect availability.

21638 - Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPZ3)

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

Risk Level: High

CVE: CVE-2017-5607

Description

Multiple vulnerabilities are present in some versions of Splunk Enterprise.

Observation

Splunk Enterprise is a platform for real-time operational intelligence.

Multiple vulnerabilities are present in some versions of Splunk Enterprise. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data or inject and store arbitrary scripts.

21558 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 52.0.1

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

Risk Level: High

CVE: CVE-2017-5428

Description

An Integer overflow vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

An Integer overflow vulnerability is present in some versions of Mozilla Firefox ESR. The flaw lies in createImageBitmap API. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system or cause a denial of service condition.

21559 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 52.0.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5428

Description

An Integer overflow vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

An Integer overflow vulnerability is present in some versions of Mozilla Firefox ESR. The flaw lies in createImageBitmap API. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system or cause a denial of service condition.

21570 - Solarwinds Log and Event Manager Two Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-5198, CVE-2017-5199

Description

Multiple vulnerabilities are present in some versions of Solarwinds Log And Event Manager.

Observation

Solarwinds Log And Event Manager is a Security Information and Event Manager software.

Multiple vulnerabilities are present in some versions of Solarwinds Log And Event Manager. The vulnerabilities lie in an incorrect sudo configuration and an editable permission on /usr/local/contego/scripts/mgrconfig.pl. Successful exploitation could allow an attacker to execute arbitrary code or escalate its privileges.

21571 - HP Intelligent Management Center Remote Unauthenticated Disclosure of Information Vulnerability

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

Risk Level: High

CVE: CVE-2017-5797

Description

An information disclosure vulnerability is present in some versions of HP Intelligent Management Center.

Observation

HP Intelligent Management Center (iMC) is an enterprise-class network management platform.

An information disclosure vulnerability is present in some versions of HP Intelligent Management Center. The flaw lies in the SOM module. Successful exploitation could result in an information disclosure.

21582 - Novell Sentinel Multiple Vulnerabilities Prior To 8.0 SP1 Build 3512

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1000031, CVE-2017-5184, CVE-2017-5185

Description

Multiple vulnerabilities are present in some versions of Novell Sentinel.

Observation

Sentinel is a security information and event management (SIEM) tool.

Multiple vulnerabilities are present in some versions of Novell Sentinel. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

21624 - IBM AIX Java Multiple Vulnerabilities (January 2017)

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

Risk Level: High

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

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 Java SDK component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

21630 - (HT207600) Apple Safari Multiple Vulnerabilities Prior To 10.1

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-9642, CVE-2016-9643, CVE-2017-2364, CVE-2017-2367, CVE-2017-2376, CVE-2017-2377, CVE-2017-2378, CVE-2017-2385, CVE-2017-2386, CVE-2017-2389, CVE-2017-2392, CVE-2017-2394, CVE-2017-2395, CVE-2017-2396, CVE-2017-2405, CVE-2017-2415, CVE-2017-2419, CVE-2017-2424, CVE-2017-2433, CVE-2017-2442, CVE-2017-2444, CVE-2017-2445, CVE-2017-2446, CVE-2017-2447, CVE-2017-2453, CVE-2017-2454, CVE-2017-2455, CVE-2017-2457, CVE-2017-2459, CVE-2017-2460, CVE-2017-2463, CVE-2017-2464, CVE-2017-2465, CVE-2017-2466, CVE-2017-2468, CVE-2017-2469, CVE-2017-2470, CVE-2017-2471, CVE-2017-2475, CVE-2017-2476, CVE-2017-2479, CVE-2017-2480, CVE-2017-2481, CVE-2017-2486

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service, conduct spoofing attacks or remotely execute arbitrary

code.

21651 - Wireshark Multiple Vulnerabilities Prior To 2.2.6

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

Risk Level: High

CVE: CVE-2017-7700, CVE-2017-7701, CVE-2017-7702, CVE-2017-7703, CVE-2017-7704, CVE-2017-7705

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

21653 - Apache Tomcat Vulnerability Prior To 7.0.77

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

Risk Level: High

CVE: CVE-2017-5647

Description

An information disclosure vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

An information disclosure vulnerability is present in some versions of Apache Tomcat. The flaw lies in the handling of the pipelined requests when send file was used. Successful exploitation could allow an attacker to obtain sensitive information.

21654 - Wireshark Multiple Vulnerabilities Prior To 2.0.12

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

Risk Level: High

CVE: CVE-2017-7700, CVE-2017-7701, CVE-2017-7702, CVE-2017-7703, CVE-2017-7705

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

21655 - Apache Tomcat Vulnerability Prior To 8.0.43

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

Risk Level: High

CVE: CVE-2017-5647

Description

An information disclosure vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

An information disclosure vulnerability is present in some versions of Apache Tomcat. The flaw lies in the handling of pipelined requests when send file is used. Successful exploitation could allow an attacker to obtain sensitive information.

21657 - Apache Tomcat Multiple Vulnerabilities Prior To 8.5.13

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

Risk Level: High

CVE: CVE-2017-5647, CVE-2017-5650, CVE-2017-5651

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information or cause denial of service condition.

21579 - (HT207607) Apple iCloud Multiple Vulnerabilities Prior To 6.2

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

Risk Level: Medium

CVE: CVE-2017-2383, CVE-2017-2463, CVE-2017-2479, CVE-2017-2480, CVE-2017-5029

Description

Multiple vulnerabilities are present in some versions of Apple iCloud.

Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

Multiple vulnerabilities are present in some versions of Apple iCloud. The flaws lie in multiple components component. Successful exploitation could allow an attacker to execute arbitrary code, cause a denial of service or obtain sensitive information.

21650 - Trend Micro Control Manager Multiple Vulnerabilities (2016-0033)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Trend Micro Control Manager.

Observation

Trend Micro Control Management is an enterprise tool provides centralized management for Threat Detection and Data Protection.

Multiple vulnerabilities are present in some versions of Trend Micro Control Manager. The flaws lie in multiple components. Successful exploitation could allow an attacker to escalate privileges, bypass security access restrictions, remotely execute arbitrary code on the target system.

21670 - Oracle Java SE Critical Patch Update April 2017

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3512, CVE-2017-3514, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

Observation

Oracle Java SE is used to run Java applications.

Multiple vulnerabilities are present in some versions of Oracle Java SE. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause application crash, obtain sensitive information or execute arbitrary code.

21568 - (K37526132) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-3731

Description

A denial of service vulnerability is present in some versions of F5 BIG-IP systems.

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in OpenSSL where a specific truncated packet could cause out-of-bounds read. Successful exploitation could allow an attacker to crash the server or client resulting in a denial of service.

21576 - Cisco Nexus 9000 Series Switches Remote Login Denial Of Service Vulnerability (CSCuy25824)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3879

Description

A denial of service vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A denial of service vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the remote login functionality.

Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

21581 - (HT207604) Apple macOS Server Multiple Vulnerabilities Prior to 5.3

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2007-6750, CVE-2016-0751, CVE-2017-2382

Description

Multiple vulnerabilities are present in some versions of Apple macOS Server.

Observation

Apple macOS Server provides easy to use interface to configure enterprise services for Apple devices.

Multiple vulnerabilities are present in some versions of Apple macOS Server. The flaws lie in the Action Pack in Ruby on Rails, Apache HTTP Server and Wiki Server components. Successful exploitation could allow an attacker to cause denial of service or to enumerate user accounts.

21625 - (CTX222565) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-10013, CVE-2017-7228

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 lie in multiple components. Successful exploitation could allow the administrator of an HVM guest VM to compromise the host.

21641 - Novell iManager Vulnerability Prior To 2.7 Support Pack 7 - Patch 10

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

Risk Level: Medium

CVE: CVE-2016-2183

Description

A vulnerability is present in some versions of Novell (NetIQ) iManager.

Observation

Novell iManager is a web-based administration console.

A vulnerability is present in some versions of Novell (NetIQ) iManager. The flaw lies in Tomcat component. Successful exploitation could allow an attacker to recover encrypted plain texts.

21644 - (VMSA-2017-0006) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4902, CVE-2017-4903, CVE-2017-4904, CVE-2017-4905

Description

Multiple vulnerabilities are present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware Fusion. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code in the context of the host.

21645 - (SB10188) McAfee ePolicy Orchestrator Multiple OpenSSL Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-7055, CVE-2017-3732

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to disclose information or cause a denial of service condition.

21652 - (SB10194) McAfee VirusScan Enterprise Memory Corruption Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8030

Description

A memory corruption vulnerability is present in some versions of McAfee VirusScan Enterprise.

Observation

McAfee VirusScan Enterprise is McAfee's anti-malware software.

A memory corruption vulnerability is present in some versions of McAfee VirusScan Enterprise. The flaw lies in the Scriptscan COM Object in McAfee VirusScan Enterprise. Successful exploitation could allow an attacker to cause a denial of service.

21656 - Cisco Adaptive Security Appliance BGP Bidirectional Forwarding Detection ACL Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3867

Description

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA).

Observation

Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA). The flaw lies in the Bidirectional Forwarding Detection (BFD) implementation. Successful exploitation could allow an attacker to bypass the ACL for some specific TCP and UDP traffic.

21660 - Microsoft Internet Information Services Buffer Overflow

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

Risk Level: Medium

CVE: CVE-2017-7269

Description

A vulnerability in some versions of Microsoft IIS could lead to a buffer overflow.

Observation

A vulnerability in some versions of Microsoft IIS could lead to a buffer overflow.

The flaw lies in the ScStoragePathFromUrl function in the WebDAV service. Successful exploitation could allow a remote attacker to execute arbitrary code.

21669 - Apache Tomcat Vulnerability Prior To 6.0.53

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

Risk Level: Medium

CVE: CVE-2017-5647

Description

An information disclosure vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

An information disclosure vulnerability is present in some versions of Apache Tomcat. The flaw lies in the handling of the pipelined requests. Successful exploitation could allow an attacker to retrieve sensitive data.

21637 - IBM WebSphere Portal Cross Site Scripting Vulnerability (swg22000152)

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

Risk Level: Medium

CVE: CVE-2017-1120

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in Web UI. Successful exploitation could allow an attacker to perform cross-site scripting attacks.

21639 - McAfee Anti-Malware Scan Engine Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-8031, CVE-2016-8032

Description

Multiple vulnerabilities are present in some versions of McAfee Anti-Malware Scan Engine.

Observation

McAfee Anti-Malware Scan Engine is an antivirus program.

Multiple vulnerabilities are present in some versions of McAfee Anti-Malware Scan Engine. The flaws are due to improper handling of crafted input files. Successful exploitation could allow a local attacker to crash the scan engine and bypass local security protection.

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.

21634 - (APSB17-11) Vulnerabilities In Adobe Reader And Acrobat

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

Risk Level: High

CVE: CVE-2017-3011, CVE-2017-3012, CVE-2017-3013, CVE-2017-3014, CVE-2017-3015, CVE-2017-3017, CVE-2017-3018, CVE-2017-3019, CVE-2017-3020, CVE-2017-3021, CVE-2017-3022, CVE-2017-3023, CVE-2017-3024, CVE-2017-3025, CVE-2017-3026, CVE-2017-3027, CVE-2017-3028, CVE-2017-3029, CVE-2017-3030, CVE-2017-3031, CVE-2017-3032, CVE-2017-3033, CVE-2017-3034, CVE-2017-3035, CVE-2017-3036, CVE-2017-3037, CVE-2017-3038, CVE-2017-3039, CVE-2017-3040, CVE-2017-3041, CVE-2017-3042, CVE-2017-3043, CVE-2017-3044, CVE-2017-3045, CVE-2017-3046, CVE-2017-3047, CVE-2017-3048, CVE-2017-3049, CVE-2017-3050, CVE-2017-3051, CVE-2017-3052, CVE-2017-3053, CVE-2017-3054, CVE-2017-3055, CVE-2017-3056, CVE-2017-3057, CVE-2017-3065

Update Details

Risk is updated

33152 - Oracle Solaris 119758-38 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-0452, CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4138, CVE-2007-4572, CVE-2007-5398, CVE-2007-6015, CVE-2008-4314, CVE-2010-2063, CVE-2010-3069, CVE-2011-0719, CVE-2011-2522, CVE-2011-2694, CVE-2012-1182, CVE-2012-2111, CVE-2012-6150, CVE-2013-0213, CVE-2013-0214, CVE-2013-4124, CVE-2013-4408, CVE-2013-4475, CVE-2013-4496, CVE-2014-0178, CVE-2014-0244, CVE-2014-3493

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33154 - Oracle Solaris 119757-38 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-0452, CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4138, CVE-2007-4572, CVE-2007-5398, CVE-

2007-6015, CVE-2008-4314, CVE-2010-2063, CVE-2010-3069, CVE-2011-0719, CVE-2011-2522, CVE-2011-2694, CVE-2012-1182, CVE-2012-2111, CVE-2012-6150, CVE-2013-0213, CVE-2013-0214, CVE-2013-4124, CVE-2013-4408, CVE-2013-4475, CVE-2013-4496, CVE-2014-0178, CVE-2014-0244, CVE-2014-3493

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

20856 - (SYM16-017) Symantec Web Gateway Management Console Interface Command Injection Vulnerability

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

Risk Level: High

CVE: CVE-2016-5313

Update Details

Risk is updated

32911 - Oracle Solaris 147993-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-4528, CVE-2011-1091, CVE-2011-2943, CVE-2011-3184, CVE-2011-3185, CVE-2011-4601, CVE-2011-4602, CVE-2011-4603, CVE-2011-4922, CVE-2011-4939, CVE-2012-1178, CVE-2012-2214, CVE-2012-2318, CVE-2012-3374

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32914 - Oracle Solaris 147992-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-4528, CVE-2011-1091, CVE-2011-2943, CVE-2011-3184, CVE-2011-3185, CVE-2011-4601, CVE-2011-4602, CVE-2011-4603, CVE-2011-4922, CVE-2011-4939, CVE-2012-1178, CVE-2012-2214, CVE-2012-2318, CVE-2012-3374

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33312 - Oracle Solaris 152078-51 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33313 - Oracle Solaris 152076-51 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33314 - Oracle Solaris 152079-51 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33315 - Oracle Solaris 152077-51 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32575 - Oracle Solaris 143506-12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-1634, CVE-2010-3492, CVE-2011-3389, CVE-2012-0845, CVE-2012-0876, CVE-2012-1150, CVE-2013-4238, CVE-2014-1912, CVE-2014-7185

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32576 - Oracle Solaris 143507-12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-1634, CVE-2010-3492, CVE-2011-3389, CVE-2012-0845, CVE-2012-0876, CVE-2012-1150, CVE-2013-4238, CVE-2014-1912, CVE-2014-7185

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

170653 - Amazon Linux AMI ALAS-2016-675 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-1908

Update Details

Risk is updated

190299 - Fedora Linux 23 FEDORA-2016-4509765b4b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1908

Update Details

Risk is updated

32622 - Oracle Solaris 143725-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-3563, CVE-2013-5211, CVE-2014-9295, CVE-2014-9296

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32623 - Oracle Solaris 143726-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-3563, CVE-2013-5211, CVE-2014-9295, CVE-2014-9296

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33145 - Oracle Solaris 150401-49 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

141212 - Red Hat Enterprise Linux RHSA-2016-1267 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

141215 - Red Hat Enterprise Linux RHSA-2016-1293 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

145116 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3250-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Update Details

Risk is updated

160112 - CentOS 6 CESA-2016-1267 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

160116 - CentOS 7 CESA-2016-1293 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

163107 - Oracle Enterprise Linux ELSA-2016-1267 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

163114 - Oracle Enterprise Linux ELSA-2016-1293 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

174978 - Scientific Linux Security ERRATA Important: setroubleshoot and setroubleshoot-plugins on SL7.x x86_64 (1606-7157)

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

174980 - Scientific Linux Security ERRATA Important: setroubleshoot and setroubleshoot-plugins on SL6.x i386/x86_64 (1606-7583)

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

Risk Level: Medium

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Update Details

Risk is updated

181686 - FreeBSD a2ps Format String Vulnerability (e359051d-90bd-11e5-bd18-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8107

Update Details

Risk is updated

181838 - FreeBSD qemu Denial Of Service Vulnerability In VMWARE VMXNET3 NIC Support (9ad8993e-b1ba-11e5-9728-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8567, CVE-2015-8568

Update Details

Risk is updated

190706 - Fedora Linux 22 FEDORA-2016-f597359bf2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4446

Update Details

Risk is updated

190823 - Fedora Linux 23 FEDORA-2016-b68f69b086 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4446

Update Details

Risk is updated

190862 - Fedora Linux 23 FEDORA-2016-f2493c754a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4446

Update Details

Risk is updated

190875 - Fedora Linux 24 FEDORA-2016-75ca94dee3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4446

Update Details

Risk is updated

190899 - Fedora Linux 24 FEDORA-2016-047a86f5b1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4446

Update Details

Risk is updated

191510 - Fedora Linux 25 FEDORA-2016-fbf9f8b204 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Update Details

Risk is updated

191578 - Fedora Linux 24 FEDORA-2016-04383482b4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Update Details

Risk is updated

191640 - Fedora Linux 25 FEDORA-2017-5bf9a268df Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Update Details

Risk is updated

191653 - Fedora Linux 24 FEDORA-2017-3d771a1702 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Update Details

Risk is updated

145147 - SuSE SLES 12 SP1, 12 SP2 SUSE-SU-2017:0102-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4680

Update Details

Risk is updated

181509 - FreeBSD freeradius Insufficent CRL Application Vulnerability (379788f3-2900-11e5-a4a5-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-4680

Update Details

Risk is updated

181693 - FreeBSD KeePassX Information Disclosure (918a5d1f-9d40-11e5-8f5c-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8378

Update Details

Risk is updated

181829 - FreeBSD qemu Denial Of Service Vulnerability In Human Monitor Interface Support (62ab8707-b1bc-11e5-9728-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8619

Update Details

Risk is updated

185577 - Ubuntu Linux 16.04 USN-3195-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5936

Update Details

Risk is updated

33162 - Oracle Solaris 150400-49 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

93424 - Mandriva Linux MBS1 MDVSA-2014-226 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716

Update Details

Risk is updated

93581 - Mandriva Linux MBS2 MDVSA-2015-105 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-1958, CVE-2014-2030, CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716

Update Details

Risk is updated

141333 - Red Hat Enterprise Linux RHSA-2016-2605 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5011

Update Details

Risk is updated

142506 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1396-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562

Update Details

Risk is updated

142560 - SuSE SLES 11 SP3, SLED 11 SP3 ImageMagick-9976 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716

Update Details

Risk is updated

143250 - SuSE SLES 12, SLED 12 SUSE-SU-2014:1595-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716

Update Details

Risk is updated

143253 - SuSE SLES 11 SP3, SLED 11 SP3 SUSE-SU-2014:1631-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716

Update Details

Risk is updated

144993 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2764-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5011

Update Details

Risk is updated

145034 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:2954-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5011

Update Details

Risk is updated

163222 - Oracle Enterprise Linux ELSA-2016-2605 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-5011

Update Details
Risk is updated

175080 - Scientific Linux Security ERRATA Low: util-linux on SL7.x x86_64 (1612-3139)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2016-5011

Update Details
Risk is updated

181949 - FreeBSD Bugzilla Security Issues (036d6c38-1c5b-11e6-b9e0-20cf30e32f6d)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2803

Update Details
Risk is updated

188957 - Fedora Linux 22 FEDORA-2015-3605 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-8354, CVE-2014-8355

Update Details
Risk is updated

189107 - Fedora Linux 21 FEDORA-2015-3612 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-8354, CVE-2014-8355

Update Details
Risk is updated

190218 - Fedora Linux 23 FEDORA-2016-105b3b8804 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-1838, CVE-2015-1839

Update Details

Risk is updated

190655 - Fedora Linux 22 FEDORA-2016-5bd283c48b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2803

Update Details
Risk is updated

190757 - Fedora Linux 23 FEDORA-2016-6cdcddef2c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2803

Update Details
Risk is updated

190837 - Fedora Linux 24 FEDORA-2016-37a8cb68c5 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2803

Update Details
Risk is updated

33336 - Oracle Solaris 152099-41 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33339 - Oracle Solaris 152097-41 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33340 - Oracle Solaris 152098-41 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33341 - Oracle Solaris 152096-41 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33349 - Oracle Solaris 152101-31 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33350 - Oracle Solaris 152100-31 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

142527 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1492-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8716

Update Details

Risk is updated

181839 - FreeBSD qemu Denial Of Service Vulnerabilities In Eepro100 NIC Support (b56fe6bb-b1b1-11e5-9728-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8345

Update Details

Risk is updated

181743 - FreeBSD qemu Denial Of Service Vulnerability In Q35 Chipset Emulation (152acff3-b1bd-11e5-9728-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8666

Update Details

Risk is updated

181835 - FreeBSD qemu Denial Of Service Vulnerability In MegaRAID SAS HBA Emulation (b3f9f8ef-b1bb-11e5-9728-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8613

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

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.