2014-APR-14

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

16511 - IMAP STARTTLS OpenSSL TLS DTLS Heartbeat Extension Packets Information Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2014-0160

Description

A vulnerability in some versions of OpenSSL could lead to information disclosure.

Observation

A vulnerability in some versions of OpenSSL could lead to information disclosure.

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness can allow an attacker to steal information that is normally protected by the SSL/TLS encryption used to secure communications on the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read portions of the memory of the systems protected by the vulnerable versions of the OpenSSL software. This may compromise the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users. (See Heartbleed.com)

Only products that use OpenSSL 1.0.1a through 1.0.1f (inclusive) are vulnerable. All of the 1.0.2 beta versions have been reported as being vulnerable too (http://info.elastica.net/2014/04/openssl-heartbeat-vulnerability/). This bug was introduced to OpenSSL in December 2011 and has been in production since OpenSSL release 1.0.1 on 14 March 2012. OpenSSL 1.0.1g, released on 7 April 2014, fixes the bug.

In addition to affecting servers, it has been reported that some clients are vulnerable as well:
https://security.stackexchange.com/questions/55249/what-clients-are-proven-to-be-vulnerable-to-heartbleed

A client test server (aka a server to test if a client is vulnerable) available at:
https://github.com/Lekensteyn/pacemaker

CVE-2014-0160
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

16512 - FTP STARTTLS OpenSSL TLS DTLS Heartbeat Extension Packets Information Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2014-0160

Description

A vulnerability in some versions of OpenSSL could lead to information disclosure.

Observation

A vulnerability in some versions of OpenSSL could lead to information disclosure.

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness can allow an attacker to steal information that is normally protected by the SSL/TLS encryption used to secure communications on the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read portions of the memory of the systems protected by the vulnerable versions of the OpenSSL software. This may compromise the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users. (See Heartbleed.com)

Only products that use OpenSSL 1.0.1a through 1.0.1f (inclusive) are vulnerable. All of the 1.0.2 beta versions have been reported as being vulnerable too (http://info.elastica.net/2014/04/openssl-heartbeat-vulnerability/). This bug was introduced to OpenSSL in December 2011 and has been in production since OpenSSL release 1.0.1 on 14 March 2012. OpenSSL 1.0.1g, released on 7 April 2014, fixes the bug.

In addition to affecting servers, it has been reported that some clients are vulnerable as well:
https://security.stackexchange.com/questions/55249/what-clients-are-proven-to-be-vulnerable-to-heartbleed

A client test server (aka a server to test if a client is vulnerable) available at:
https://github.com/Lekensteyn/pacemaker

CVE-2014-0160
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

16513 - POP3 STARTTLS OpenSSL TLS DTLS Heartbeat Extension Packets Information Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2014-0160

Description

A vulnerability in some versions of OpenSSL could lead to information disclosure.

Observation

A vulnerability in some versions of OpenSSL could lead to information disclosure.

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness can allow an attacker to steal information that is normally protected by the SSL/TLS encryption used to secure communications on the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read portions of the memory of the systems protected by the vulnerable versions of the OpenSSL software. This may compromise the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users. (See Heartbleed.com)

Only products that use OpenSSL 1.0.1a through 1.0.1f (inclusive) are vulnerable. All of the 1.0.2 beta versions have been reported as being vulnerable too (http://info.elastica.net/2014/04/openssl-heartbeat-vulnerability/). This bug was introduced to OpenSSL in December 2011 and has been in production since OpenSSL release 1.0.1 on 14 March 2012. OpenSSL 1.0.1g, released on 7 April 2014, fixes the bug.

In addition to affecting servers, it has been reported that some clients are vulnerable as well:
https://security.stackexchange.com/questions/55249/what-clients-are-proven-to-be-vulnerable-to-heartbleed

A client test server (aka a server to test if a client is vulnerable) available at:
https://github.com/Lekensteyn/pacemaker

CVE-2014-0160
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

16444 - IBM WebSphere Portal WCM Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6328

Description

A cross-site scripting vulnerability exists 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 cross-site scripting vulnerability exists in some versions of IBM WebSphere Portal. A flaw is present in wcm.path.traversal.security setting. Successful exploitation could allow an attacker to inject arbitrary web script.

16510 - WordPress Marekkis Watermark Plugin "pfad" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-1758

Description

A cross site scripting vulnerability is present in some versions of WordPress Marekkis Watermark.

Observation

WordPress is a popular blog web application. Marekkis Watermark is a plugin for WordPress that adds watermarks to pictures.

A cross site scripting vulnerability is present in some versions of WordPress Marekkis Watermark.The flaw lies in the plugin's pfad parameter which the plugin fails to verify its input. Successful exploitation could allow an attacker to execute arbitrary code within the user's browser.

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.

4615 - Administrator Users Password Never Expires

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

Risk Level: High

Check Version: 1.1356

CVE: CVE-1999-0535

Update Details

FASLScript is updated.

14804 - IOServer OPC Server Denial of Service

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

Risk Level: High

CVE: CVE-2013-2783

Update Details

Recommendation is updated.
Risk is updated.

16426 - Linksys Multiple E-Series Routers Security Bypass Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

CVE: CVE-2013-5122

Update Details

Recommendation is updated.

16505 - OpenSSL TLS DTLS Heartbeat Extension Packets Information Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2014-0160

Update Details

FASLScript is updated.

16384 - Cisco Adaptive Security Appliance Phone Proxy CTL Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0738

Update Details

Recommendation is updated.

16465 - Kaspersky Internet Security Regular Expression Patterns Processing Denial of Service Vulnerability

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

Risk Level: Medium

Update Details

Recommendation is updated.

ADDITIONAL NOTES

16505 - is now including extra TCP ports for better vulnerability detection.

16511, 16512, 16513 - were created to detect heartbleed over secure IMAP, FTP and POP3 implementation(STARTTLS).

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.