Server Automation Alert:

SSL/TLS MITM Vulnerability Update
CVE-2014-0224

(December 22, 2014)

Call for Action

Information in this document applies to multiple releases from 9.1x up to 10.1. For SA version 10.1 or later, no action is needed, as that version uses OpenSSL version 1.0.1h, and, therefore, CVE-2014-0024 does not apply. Earlier SA releases use OpenSSL version 0.9.8, and this version of OpenSSL has only a part of the defect found in OpenSSL version 1.0.1. Security researchers have been unable to prove that the defect in OpenSSL 0.9.8 is exploitable. HP is monitoring the issue's impact, but does not recommend any action at this time. As a pre-emptive measure, you may choose to upgrade to SA version 10.1 or later, which completely resolves the CVE-2014-0224 vulnerability. If the situation changes, this bulletin will be updated with the new information.

Important: The Heartbleed patch SRV_00177 must be installed for the SA Software Repository Download Accelerator (Tsunami) for SA 10.0 and 10.01.

Contents

Change Table for this Document

Date	Change
October 4, 2014	Initial Release
December 22, 2014	Updated reference to "10.1" to say "10.1 or later"

Reason for This Update

Previous HP SA Security Alerts, for example, http://support.openview.hp.com/selfsolve/document/LID/SRVA_00177, dealt with other SSL/TLS MITM vulnerabilities, and called for appropriate actions to mitigate them. Other third-party alerts (for example, https://www.openssl.org/news/secadv_20140605.txt) dealt with other OpenSSL vulnerabilities, but only one of those applies to SA. The present bulletin was issued to add further details about the OpenSSL vulnerability.

Issue that Requires Attention

CVE-2014-0224 is a vulnerability found in the OpenSSL cryptographic software library. This vulnerability can only be exploited between vulnerable clients and servers.

The vulnerability allows an attacker to:

1. Use a carefully crafted handshake to exploit weak keying material.
2. Perform Man-in-the-middle (MITM) attacks, where traffic from vulnerable clients and servers can be modified and decrypted.

Who is affected?

You will be affected by this vulnerability if you use any web server, application server, or operating system that uses or includes affected versions of OpenSSL libraries.

What OpenSSL and SA Versions are Vulnerable?

The following table shows recent SA versions and their corresponding OpenSSL versions. SA versions that use OpenSSL 1.0.1h are not vulnerable to CVE-2014-0224.

SA Version	OpenSSL Version
9.10 through 9.16	0.9.8g for all components.
10.0 and 10.01	1.0.1h for the SA Software Repository Download Accelerator (Tsunami) if you applied the Heartbleed patch SRV_00177. 0.9.8g for all components.
10.02	1.0.1h for the SA Software Repository Download Accelerator (Tsunami), all other components use 0.9.8g.
10.10	1.0.1h for all components.

Relevant OpenSSL Vulnerability Information from Other Sources

Different security bulletins (from a number of sources) provide information on the OpenSSL vulnerability. The following table describes the relevant sections in those third-party bulletins.

Bulletin Source	Relevant Information
opensl.org	https://www.openssl.org/news/secadv_20140605.txt The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1. Users of OpenSSL servers earlier than 1.0.1h are advised to upgrade as a precaution.
MITRE	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224 OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.
Lepidium (Original reporter)	http://ccsinjection.lepidum.co.jp/ Attackers can eavesdrop and falsify your communications when both a server and a client are vulnerable, and the OpenSSL version of the server is 1.0.1 or higher.

- https://www.openssl.org/news/secadv_20140605.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
- http://ccsinjection.lepidum.co.jp/
- https://www.imperialviolet.org/2014/06/05/earlyccs.html
- http://support.openview.hp.com/selfsolve/document/KM00843314/binary/SA_Alert_Heartbleed_Vulnerability.pdf
- http://support.openview.hp.com/selfsolve/document/LID/SRVA_00177