SECURITY BULLETIN - Multiple CVEs Relating to OpenSSL – Bulletin Version 1.2

Security Advisory Relating to Multiple OpenSSL Vulnerabilities on Various Polycom Products.

DATE PUBLISHED: October 4, 2014

This information applies to all Polycom products running OpenSSL versions 0.9.8 through 0.9.8y, 1.0.0 through 1.0.0l (lowercase L), 1.0.1 through 1.0.1g.

Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this bulletin has been repaired against that vulnerability. The newest version of this document will always reside at the following URL:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Vulnerability Summary

Vulnerabilities in OpenSSL could allow a remote attacker to expose sensitive data, inject data across sessions, or perform a denial of service.

Details

SSL/TLS MITM vulnerability

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.

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 1.0.1 are advised to upgrade as a precaution.

This exploit is consistent with CVE-2014-0224.

DTLS recursion flaw

By sending an invalid DTLS handshake to an OpenSSL DTLS client the code can be made to recurse eventually crashing in a DoS attack. Only applications using OpenSSL as a DTLS client are affected.

This exploit is consistent with CVE-2014-0221.

DTLS invalid fragment vulnerability

A buffer overrun attack can be triggered by sending invalid DTLS fragments to an OpenSSL DTLS client or server. This is potentially exploitable to run arbitrary code on a vulnerable client or server. Only applications using OpenSSL as a DTLS client or server affected.

This exploit is consistent with CVE-2014-0195.

SSL_MODE_RELEASE_BUFFERS NULL pointer dereference

A flaw in the do_ssl3_write function can allow remote attackers to cause a denial of service via a NULL pointer dereference. This flaw only affects OpenSSL 1.0.0 and 1.0.1 where SSL_MODE_RELEASE_BUFFERS is enabled, which is not the default and not common.

This exploit is consistent with CVE-2014-0198.

SSL_MODE_RELEASE_BUFFERS session injection or denial of service

A race condition in the ssl3_read_bytes function can allow remote attackers to inject data across sessions or cause a denial of service. This flaw only affects multithreaded applications using OpenSSL 1.0.0 and 1.0.1, where SSL_MODE_RELEASE_BUFFERS is enabled, which is not the default and not common.

This exploit is consistent with CVE-2010-5298.

Anonymous ECDH denial of service

OpenSSL TLS clients enabling anonymous ECDH ciphersuites are subject to a denial of service attack.

This exploit is consistent with CVE-2014-3470.

ECDSA NONCE side-channel recovery attack

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

This exploit is consistent with CVE-2014-0076.

Products Affected

Note that the only products in this table are the products confirmed by Polycom to be fixed against the vulnerabilities in this bulletin, or confirmed by Polycom to be unaffected by the vulnerabilities in this bulletin. All other products are still under investigation.

RealPresence Distributed Media Application (DMA)	**Not Vulnerable**
RealPresence Media Manager	**Not Vulnerable**
RealPresence Capture Station	**Not Vulnerable**
CSS Gateway	**Not Vulnerable**
RealPresence Resource Manager (RPRM)	**Not Vulnerable**
CMA	**Not Vulnerable**
CX Video Products Other Than CX5500	**Not Vulnerable**
RealPresence Mobile (RPM)	**FIXED by Version 3.2.1**
RealPresence Desktop (RPD)	**FIXED by Version 3.2.1**
M100	**FIXED by Version 1.0.7**
CMAD	**FIXED by Version 5.2.6**
CSS	**FIXED by Version 1.3.1**
Group Series	**FIXED by Version 4.1.4**
Video Border Proxy (VBP)	**FIXED by Version 11.2.18**
RSS 4000	**FIXED by Version 8.5.2**
Polycom Touch Control (PTC)	**FIXED by Version 4.1.4**
HDX	**FIXED by Version 3.1.5**
VVX & SoundStructure	**FIXED by Version 5.1.2.1801**
SoundPoint & SoundStation	**FIXED by Version 4.0.7.2514**
Group Series & Polycom Touch Control	**FIXED by Version 4.1.4**
CloudAXIS Edge Service & Edge Experience Portals	**FIXED by Version 1.6.1**
RSS 4000	**FIXED by Version 8.5.2**
Capture Server	**FIXED by Version 1.7**
CX 5100/5500	**FIXED by Version 1.1.1**
RPAD	**FIXED by Version 4.0.1**
CSS Server & Client	**FIXED by Version 1.3.1**
RMX 4000/2000/1500	**FIXED by Version 8.4.1**
RMX 1800/Collaboration Server, Virtual Edition	**FIXED by Version 8.4.1**
Platform Director	**Under Investigation**

Mitigation

Polycom recommends that customers use the latest versions of OpenSSL clients (0.9.8za, 1.0.0m, and 1.0.1h) to protect against CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-3470, and CVE-2014-0076.

In addition, Polycom recommends that customers evaluate network access control lists, firewalls and other network protections to ensure that they have been deployed in a manner that is consistent with security best practices. The risk presented by this potential vulnerability to Polycom products, as well as other networked devices, may be mitigated by these controls. Customers should also ensure that Polycom products have been configured as recommended by Polycom implementation guides. Customers may wish to implement additional event monitoring and review until such time that an update is installed.

Solution

As fixes become available for a given product, that information will appear in this bulletin in subsequent releases. Polycom will continue updating this bulletin until all fixes are in place. Polycom recommends that users of any Polycom product listed in the table above as being vulnerable update to the “FIXED” version of their product as soon as such a version becomes available.

CVSS v2 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom leverages the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v2 Scores:

CVE-2010-5298: 4.0 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2014-0195: 6.8 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2014-0198: 4.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2014-0221: 4.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2014-0224: 6.8 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2014-3470: 4.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2014-0076: 4.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

For more information on CVSS v2 please see:
http://www.first.org/cvss/cvss-guide.html

Severity: Medium

Rating	Definition
Critical	A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.
High	A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of

	data, or of the integrity or availability of resources.
Medium	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
Low	A vulnerability that has minimal impact to the system and is extremely difficult to exploit.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

for the latest information. You might also find value in the high-level security guidance and security news located at:

http://www.polycom.com/security

Revision History

Revision 1.0 - Original publication: June 30, 2014 – VBP Fix Announced
Revision 1.1 – Original publication: August 5, 2014 – RPM, RPD, M100, CMAD, CSS, Group Series announced

Revision 1.2 – Original publication: September 15, 2014 – HDX,