SECURITY ADVISORY – “Logjam” (CVE-2015-4000)
Advisory Version 1.6.1

Security Advisory Relating to “Logjam” Vulnerability on Various Polycom Products.

DATE PUBLISHED: October 23nd, 2015

Polycom is conducting ongoing research to determine the level of vulnerability (if any) for each of its various products.

Any information in this advisory is subject to change and additional information will be added as it becomes available.

Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this advisory 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

A vulnerability has been recently disclosed in the way Diffie-Hellman key exchanges take place. This vulnerability could potentially allow a “man-in-the-middle” attacker to downgrade the strength of a TLS connection to a weaker 512-bit, export-grade cryptography. The vulnerability is known as “Logjam” and has been assigned the following CVE identifier:

CVE-2015-4000: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000

Details

CVE-2015-4000, aka “Logjam”

Logjam Attack against the TLS Protocol. The Logjam attack allows a “man-in-the-middle” attacker to downgrade TLS connections to 512-bit, export-grade cryptography. The attack leverages the Diffie-Hellman key exchange and exploits a flaw in the TLS protocol, forcing a downgrade in cryptography. As with other vulnerabilities of its kind (POODLE & FREAK), the exploit requires that the attacker be on the same network as the target.

Mitigations

There are no specific mitigations at this time for this vulnerability. Security best practices should be followed and some recommendations can be found at:

http://www.polycom.com/content/dam/polycom/www/documents/white-papers/polycom-uc-security-best-practices-wp-enus.pdf

Products Affected

Note that the products listed in the below table are the only products whose vulnerability status can be definitively stated at this time – to the positive or the negative. Any products not listed in this chart remain under investigation, and will appear in this chart as soon as their status is known.

Media Manager – All Versions	Not Vulnerable
CX5000 – All Versions	Not Vulnerable
Video Border Proxy (VBP) – All Versions	Patches available - 11.2.23 and 14.2.0.1
CX Product Line, All Other Video Versions	Not Vulnerable
RealPresence Desktop – All Versions	Fix coming in 3.5 - December
Group Series – All Versions	Not Vulnerable
Real Presence Capture Server	Fix coming in 2.5
RealPresence Access Director (RPAD) – All Versions	Web Fixed in 4.2.1, SSH can be disabled with future fix coming
CloudAXIS MEA – All Versions	Fix coming in 2.1 – December
CloudAXIS WSP – All Versions	Fix coming in 2.1 - December
Platform Director – All Versions	Fixed in 2.0
HDX – All Versions	Not Vulnerable
RealPresence Resource Manager (RPRM)	Fix coming in 9.0* - December
RSS 4000 – All Versions	Investigating
Distributed Media Application (DMA) – All Versions	Web UI not vulnerable, SSH can be disabled with future fix coming in 9.0*
Content Sharing Suite Client/Server – All Versions	Fix coming in 1.5.1 - December
RealPresence Collaboration Server (RMX) – All Versions	Fix available in 8.6.2 and 8.5.4
RealPresence Mobile – All Versions	Fix coming in 3.5 - December
UC Phones – VVX - All Versions	Not Vulnerable
UC Phones – SPIP & SSIP – All Versions	Not Vulnerable

** Some products are shifting software versions to 9.0 from lower version numbers*

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-2015-4000: 4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N

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: May 21, 2015 – First Announcement
Revision 1.1 – May 22, 2015: More clarity on local network requirements to exploit
Revision 1.2 – May 29, 2015: Updated severity to align with CVSS score
Revision 1.3 – July 16, 2015: Updated product information
Revision 1.4 – August 1, 2015: updated release versions
Revision 1.5 – September 30, 2015: Updated release versions
Revision 1.6 – October 22, 2015: Updated release versions and dates
Revision 1.6.1 – October 23, 2015: Added note regarding version number shift