SECURITY BULLETIN CVE-2014-0160 Version 1.5

Security Advisory Relating to OpenSSL Vulnerability "Heartbleed" on Various Polycom Products

DATE PUBLISHED: 2014-04-17-12:38 Texas Time

This information applies to all Polycom products using OpenSSL versions 1.0.1 through 1.01f.

Summary

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.

Details

Through exploiting the heartbeat feature in OpenSSL versions 1.0.1 through 1.0.1f, an attacker can capture memory from the host 64k at a time. Successive 64k sections of memory can be captured until the attacker has captured the desired data. This could include, at worst case, a copy of the server's private key.

This exploit is consistent with CVE: 2014-0160

Systems Affected

At this time, a nearly complete list of Polycom products, their versions, and vulnerability status is outlined in the table below. This bulletin will be updated periodically until all Polycom products/versions are known to be vulnerable or not, and until all vulnerable systems are fixed or properly mitigated. **NOTE: Any dates listed in the table below are ESTIMATES. These dates are subject to change, for better or worse, as new information becomes available to the teams in charge of each product.**

Product Name	Version	Vulnerable	Notes and/or FIX/FIXED Dates
Management Applications			
CMA			

CMA	All	Not Vulnerable	
RealPresence Distributed Media Application (DMA)			
DMA	All	Not Vulnerable	
RealPresence Resource Manager (RPRM)			
RPRM	7.1	Not vulnerable	
RPRM	7.3	Not vulnerable	
RPRM	8.x	Not vulnerable	
RealPresence Video DualManager 400			
RPDM	All	Not vulnerable	
Telepresence Rooms			
VSX Series			
VSX	All	Not Vulnerable	
HDX Series			
HDX	2.7.0.x - 3.0.x	Not Vulnerable	
HDX	3.1.x and Greater	Vulnerable	Current estimate for fix is 4/18
QDX			
QDX 6000	All	Not Vulnerable	
RealPresence Group Series			
GroupSeries	All	Vulnerable	Current estimate for fix

			is 4/23
Unified Conference Station			
CX5100 Unified Conference Station	**1.0.662**	**Not Vulnerable**	**No TLS/DTLS Server**
Desktop Video Conferencing			
RealPresence Desktop			
RPD/RPM	**All Versions**	**Not vulnerable**	
CMA Desktop			
CMAD	**All Versions**	**Not vulnerable**	
m100	**All Versions**	**Not vulnerable**	
Collaboration Servers			
RealPresence Collaboration Server 1500, 1800, 2000 and 4000 (RMX)			
RMX	**7.5.x - 7.8.x**	**Not Vulnerable**	
RMX	**8.1.4.J**	**Vulnerable**	**Best Fix Estimate Is Currently April 23, 2014**
RMX	**8.1.4.x**	**Vulnerable**	**Best Fix Estimate Is Currently April 23, 2014**
RMX	**8.1.7.x**	**Vulnerable**	**Best Fix Estimate Is Currently April 23, 2014**
RMX	**8.2.x**	**Vulnerable**	**Best Fix Estimate Is Currently April 23, 2014**
RMX	**8.3.x**	**Vulnerable**	**Best Fix Estimate Is Currently April 23, 2014**
RealPresence Collaboration Server, Virtual Edition			
SoftMCU	**8.3.x**	**Not vulnerable**	

Video Content Management			
Recording and Streaming Server (RSS) 4000			
RSS	**6.9.x**	**Not vulnerable**	
RSS	**6.9.J**	**Not vulnerable**	
RSS	**7.0.x**	**Not vulnerable**	
RSS	**7.1.x**	**Not vulnerable**	
RSS	**8.0.x**	**Not vulnerable**	
RSS	**8.5**	**Not vulnerable**	
RSS	**8.5.1**	**Not vulnerable**	
RealPresence Capture Server			
Capture Server	**1.0**	**Not vulnerable**	
Capture Server	**1.6.0**	**Not vulnerable**	
RealPresence Capture Station Pro			
Capture Station Pro	**All**	**Not vulnerable**	
RealPresence Capture Station Portable Pro			
Capture Station Portable Pro	**All**	**Not vulnerable**	
RealPresence Media Manager			
Media Manager	**All**	**Not vulnerable**	
Media Editor	**All**	**Not vulnerable**	

CSS Client			
CSS Client	All Versions	Not vulnerable	
CSS Server			
CSS Server	1.0	Not vulnerable	
CSS Server	1.1	Not vulnerable	
CSS Server	1.2	Not vulnerable	
CSS Server	1.3	Not vulnerable	
Firewall Traversal & Security			
Video Border Proxy (VBP) E Series			
VBP	11.1.x	Not vulnerable	
VBP	11.2.11 - Hotfix	Not vulnerable	
VBP	11.2.12 - GA	Vulnerable	FIXED with version 11.2.17!
VBP	11.2.16 - GA	Vulnerable	FIXED with version 11.2.17!
VBP	11.2.17	Not vulnerable	Fixes Earlier Vulnerable Versions!!!
RealPresence Access Director (RPAD)			
RPAD	1.x	Not vulnerable	
RPAD	2.x	Not vulnerable	
RPAD	3.x	Not vulnerable	
RPAD	4.x	Not vulnerable	

CloudAXIS			
CloudAXIS MEA (Web experience portal)			
CloudAXIS MEA	**All Versions**	**Not vulnerable**	
CloudAXIS WSP (Web service portal)			
CloudAXIS WSP	**All Versions**	**Not vulnerable**	
RealPresence Platform Director			
Platform Director	**1.5.0**	**Not vulnerable**	
Platform Director	**1.6.0**	**Not vulnerable**	
Voice Products			
Desktop Video & Voice Solutions			
ip430/VVX1500	**UCS 4.0.1.13681 rts56 - UCS 4.0.5.4233 rts22**	**Not Vulnerable**	
SoundPoint IP321, SoundPoint IP331, SoundPoint IP335, SoundPoint IP235T, SoundPoint IP450, SoundPoint IP550, SoundPoint IP560, SoundPoint IP650, SoundPoint IP670, SoundStation IP7000, SoundStation Duo, SoundStation IP5000,	**UCS 4.0.1.13681 rts56 - UCS 4.0.5.4233 rts22**	**Not Vulnerable**	

SoundStation IP6000, VVX500, VVX1500 and SoundStructure VoIP Interface			
SoundPoint IP430, SoundPoint IP550, SoundPoint IP560, SoundPoint IP650, SoundPoint IP320, SoundPoint IP330, SoundPoint IP321, SoundPoint IP331, SoundPoint IP335, SoundPoint IP235T, SoundPoint IP450, SoundStation IP7000, SoundStation IP5000, SoundStation IP6000, VVX1500	UCS 3.3.0.1098 rts35 - UCS 3.3.4.0085 rts6	Not Vulnerable	
SoundPoint IP550, SoundPoint IP560, SoundPoint IP650, SoundPoint IP320, SoundPoint IP330, SoundPoint IP321, SoundPoint IP331, SoundPoint IP335, SoundPoint IP235T, SoundPoint IP335, SoundPoint IP235T, SoundPoint IP450, SoundStation IP7000, SoundPoint IP430, SoundStation IP5000, SoundStation IP6000 and VVX1500	SIP 3.2.0 rts44 - SIP 3.2.7.0198 rts10	Not Vulnerable	

SoundPoint IP321, SoundPoint IP331, SoundPoint IP335, SoundPoint IP235T, SoundPoint IP450, SoundPoint IP550, SoundPoint IP560, SoundPoint IP650, SoundStation Duo, SoundStation IP5000, SoundStructure VoIP Interface	**UCS 4.1.0.84959 rts42 I - UCS 4.1.6.4835 rts50**	**Vulnerable**	**No estimate yet, but estimate should arrive on April 18. See Mitigations Section As Well.**
VVX 300/310/400/410/500/600/1500 SoundStructure VoIP Interface	**UCS 4.1.3.7864 rts21G - UCS 5.0.1.7396 rts56 Q**	**Vulnerable**	**No estimate yet, but estimate should arrive on April 18. See Mitigations Section As Well.**
Zero Touch Provisioning Solution - ZTP	**User Portal**	**No Longer Vulnerable**	***** FIXED on April 11th *****
Accessories			
TouchControl (PTC)	**All**	**Not vulnerable**	
Polycom Communicator	**All**	**Not Vulnerable**	
Other			
SoftRPP	**Unknown**	**Unknown**	
CX Series Phones			
CX500		**Unknown**	**Most likely not vulnerable - answers coming soon**
CX600		**Unknown**	**Most likely not vulnerable - answers coming soon**
CX3000		**Unknown**	**Most likely not vulnerable - answers coming soon**
CX100	**All**	**Not vulnerable**	

CX300	**All**	**Not vulnerable**	

Mitigation

At this time, many affected products have older versions to which you can temporarily regress (install older version). If you can temporarily run an older product version, this is recommended.

For some products, mitigations exist solely in the realm of controlling the presence of encrypted traffic on any system that uses a vulnerable version of OpenSSL. Basic suggestions at this time are to:

1. *Place the Polycom product behind a firewall whenever possible, such that outsiders do not have access to ports used by OpenSSL on the device (usually only HTTPS, but sometimes other protocols that use TLS such as secure LDAP or secure SIP are involved).*
2. *Turn off any services that use OpenSSL (if relevant) if at all possible. When new fixes become available, new certificates can be issued for your system, thus occluding any knowledge an attacker might have gained with regards to your old encryption certificates or keys.*

For the voice products currently listed as vulnerable, a mitigation specific to these products is available: Set your http.enabled flag to = 0 (zero). This disables web access of all kinds, and blocks known heartbeat vectors into the system.

Note that Polycom's Product Security Office is working rapidly and efficiently to assist product teams in delivering fixes in as rapid a manner as possible.

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 Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	**Low**	**None**	**Partial**	**None**	**None**

Severity: High

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 log a ticket online at:

http://www.polycom.com/security (Polycom Security Homepage) for high-level guidance, and:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html (Polycom Security Center) for specific updates.

Please remember that this bulletin is being updated on a regular basis to address new information regarding vulnerabilities and new fixes. This bulletin is versioned and time stamped.

Acknowledgment

Polycom discovered this vulnerability through the CVE database.

Revision History – Security Bulletin CVE-2014-0160

Version 1.0	2014-04-09-15:20	Initial release with 90% complete list of products and their vulnerability status
Version 1.1	2014-04-10-20:00	More detail for more products and first estimates for fix dates. Improved mitigation detail.
Version 1.2		More products, better detail, better listings for affected members of Soundpoint family

Version 1.3		Product list condensation (“versions older than”). HDX and Group Series fix date estimates published. Incorrect mitigation advice for RMX posted.
Version 1.4		More condensation and accuracy. Mitigation advice removed from RMX.
Version 1.5		RMX estimate for fix date, HDX fix date estimate moved in, mitigation for those members of Soundpoint family affected