Security Bulletin – “Tomcat Denial of Service Vulnerability” (CVE-2014-0230)
Bulletin Version 1.0

Security Bulletin Relating to “Tomcat Denial of Service” Vulnerability on Various Polycom Products.

DATE PUBLISHED: June 17th, 2015

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

Any information in this bulletin 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 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

Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (memory consumption) via a series of aborted upload attempts. The vulnerability has been assigned the following CVE identifier:

CVE-2014-0230: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0230

Details

CVE-2014-0230

From Apache Tomcat:
“When a response for a request with a request body is returned to the user agent before the request body is fully read, by default Tomcat swallows the remaining request body so that the next request on the connection may be processed. There was no limit to the size of request body that Tomcat would swallow.

This permitted a limited Denial of Service as Tomcat would never close the connection and a processing thread would remain allocated to the connection."

http://tomcat.apache.org/security-8.html

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
CMAD (CMA Desktop) – All Versions	Not Vulnerable
CX5000 – All Versions	Not Vulnerable
Video Border Proxy (VBP) – All Versions	Investigating
CX Product Line, All Other Video Versions	Not Vulnerable
RealPresence Desktop – All Versions	Not Vulnerable
Group Series – All Versions	Not Vulnerable
Capture Station – All Versions	Investigating
RealPresence Access Director (RPAD) – All Versions	Investigating
CloudAXIS MEA – All Versions	Investigating
CloudAXIS WSP – All Versions	Investigating
Platform Director – All Versions	Investigating
HDX – All Versions	Not Vulnerable
RealPresence Resource Manager (RPRM)	Investigating
RSS 4000 – All Versions	Investigating
Distributed Media Application (DMA) – All Versions	Investigating
Capture Server	Investigating
Content Sharing Suite Client/Server – All Versions	Investigating
RealPresence Collaboration Server (RMX) – All Versions	Investigating
RealPresence Mobile – All Versions	Not Vulnerable
UC Phones – VVX - All Versions	Not Vulnerable
UC Phones – SPIP & SSIP – All Versions	Not Vulnerable

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: 6.8 (AV:N/AC:L/Au:S/C:N/I:N/A:C)

For more information on CVSS v2 please see:

http://www.first.org/cvss/cvss-guide.html

Severity: High

Note: The National Vulnerability Database rates this vulnerability as a 7.8 due to its general ease of execution. On Polycom products, the attacker would need to log into the product before being able to attempt the exploit. Given this increase in difficulty, Polycom is treating the severity as if it were a 6.8.

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0230

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 17th, 2015 – First Announcement