SECURITY BULLETIN – CVE-2017-5638 “Apache Struts” – Bulletin Version 1.0

Security Bulletin Relating to *CVE-2017-5638 “Apache Struts”* Vulnerability and Polycom Products

DATE PUBLISHED: March 21st, 2017

This information applies to the Apache Struts vulnerability and Polycom products. This document is an information bulletin and thus does not contain a table of Polycom products and versions. This omission is intentional, as there is no known Apache Struts vulnerability in any Polycom system at this time.

Any information in this bulletin is subject to change.

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

The Apache Software Foundation publicly announced on March 6th, a new remote code execution (RCE) vulnerability in Apache Struts 2, an open source software framework. Polycom products do not contain Apache Struts 2 and therefore are not vulnerable to this CVE.

Vulnerability Details

CVE-2017-5638, aka “Apache Struts”

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.

Impact and Risk

There is no risk from CVE-2017-5638 in Polycom products.

Solution

Polycom products are not vulnerable to the Apache Struts vulnerability reported in CVE-2017-5638 and no action is needed.

CVSS v3 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 v3 Scores:

CVE-2017-5638: 9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

For more information on CVSS v3 please see: https://www.first.org/cvss

Severity: Critical

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

Note

Effective January 1, 2014, the below applies to all Polycom security publications:

Polycom may at times issue either a ***Security Advisory*** or a ***Security Bulletin*** with regards to a particular vulnerability or set of vulnerabilities. If a ***Security Advisory*** is issued, this means that one more Polycom products are verified by Polycom to be affected by one or more vulnerabilities. If a ***Security Bulletin*** is issued, Polycom is providing its customers with information about one or more vulnerabilities that have not been found by Polycom to directly affect any Polycom products, but that may be mistakenly thought to affect Polycom products. A ***Security Advisory*** might also be issued when a customer's environment might be affected, when false positives might occur from vulnerability scans, or when any other possible (but not actual) concern might exist regarding Polycom products and the vulnerability.

Revision History

Revision 1.0 - Original publication: March 21st, 2017

document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical Bulletin.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.