SECURITY BULLETIN – Stored Cross-Site Scripting Found in Trio – Bulletin Version 1.0

Security Bulletin Related to Stored Cross-Site Scripting Vulnerability Found in Trio

DATE PUBLISHED: November 1st, 2018

Any information in this Bulletin is subject to change.

Please Note: This is a living document and may be subject to updates. The newest version of this document can be found at the following URL:

https://support.polycom.com/content/support/security-center.html

Vulnerability Summary

A stored cross-site scripting (XSS) vulnerability was identified in the Polycom Trio admin interface. This requires physical access to the device to exploit the vulnerability.

Products Affected

Trio 8500 phones running software versions earlier than 5.5.4 contains stored stored cross-site scripting (XSS) vulnerability in the admin interface.

Solution

Update Trio 8500 phones to run software version 5.7.2 or later from the following URL:

https://support.polycom.com/PolycomService/home/home.htm

Recognition

Polycom appreciates and values the members of the security research community who find vulnerabilities, bring them to our attention, and work with Polycom in a coordinated effort so that security fixes can be issued to all impacted customers. We would like to thank the independent security researcher **Phil Wilcox** from **Cyberis Ltd.** for discovering this vulnerability, alerting us, and for cooperative disclosure.

CVSS v3 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom uses 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-2018-14935 6.1 (CVSS:3.0/AV:P/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)

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

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 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: November 01, 2018