SECURITY ADVISORY – Information Disclosure in Multiple Products - Version 1.0

Security Advisory Relating to Information Disclosure Vulnerability on Polycom UCS-Based Products

DATE PUBLISHED: August 21, 2017

Any information in this advisory 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

A medium-severity vulnerability has been discovered in the web application functionality of Polycom's UCS ("Unified Communications Software"). This vulnerability could allow an authenticated remote attacker to read a limited segment of the Polycom product's memory, which could reveal an administrator password or other sensitive information.

Impact and Risk

A non-admin user of Polycom voice products may be able to read a segment of the Polycom product's memory. This could reveal an administrator password, granting the non-admin user admin privileges.

Products Affected

SoundStation IP	Fixed in UCS version 4.0.12
VVX	Fixed in UCS version 5.6.0, 5.5.2, and 5.4.7
RealPresence Trio	Fixed in UCS version 5.4.5 rev AG

Solution

Update to the latest version of UCS for your SoundStation IP, VVX, and Trio devices.

Mitigations

Polycom recommends following standard best practices for Unified Communications, as detailed in our best practices paper found at:

http://support.polycom.com/global/documents/support/documentation/polycom_uc_security_best_practices_2015.pdf

Recognition

An independent security researcher, Francis Alexander, has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program, who in turn alerted Polycom. Polycom thanks Francis and Beyond Security for disclosing this vulnerability to us in a responsible manner.

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 Score:

5.3 - CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

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

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: August 21, 2017