SECURITY ADVISORY – UC Software - Remote Code Execution Vulnerability

Advisory Version 1.2

DATE PUBLISHED: December 20th, 2019

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

Please Note: Poly takes the security of our customers and our products seriously. This is a living document and may be subject to updates. The latest version of this document can be found at the following URL:

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

Vulnerability Summary

A vulnerability in the web-based management interface of VVX, Trio, SoundStructure, SoundPoint, and SoundStation phones running Polycom UC Software, if exploited, could allow an authenticated, remote attacker with admin privileges to cause a denial of service (DoS) condition or execute arbitrary code.

CVE-2019-12948

Products Affected

This vulnerability affects VVX, Trio, SoundStructure, SoundPoint, and SoundStation products when the web management interface is enabled.

Solution

Poly has released firmware updates to address this vulnerability. Skype for Business deployments should ensure that the appropriate BToE application is also deployed.

Products	Fix
VVX300, VVX310, VVX400, VVX410, VVX500 and VVX600	Update to : • UCS 5.8.5.1256 • UCS 5.9.3.2857 rev G • UCS 5.9.4 or later (to be released)

VVX201, VVX301, VVX311, VVX401, VVX411, VVX501 and VVX601 VVX150, VVX250, VVX350, VVX450. SoundStructure	Update to : • UCS 5.8.5.1256 • UCS 5.9.3.2857 rev G • UCS 6.0.0.4839 rev C • UCS 6.1.0 or later (to be released)
Trio	Update UCS software to version 5.9.0 Rev AD or later
SoundPoint and SoundStation	Update to: • UCS 4.0.14.1580 • UCS 4.1.1.0934 rts11 AB

https://support.polycom.com/content/support/north-america/usa/en/support/voice/polycom-uc/polycom-uc-software-release.html

Mitigation

In addition, as a further mitigation and aligned with standard security best practices, Poly also recommends that customers change the Admin password on the phones from a default or weak password to a strong (minimum 10 character) password. This mitigation limits the ability of the attacker to compromise the phone and is the quickest measure that can be taken to reduce risk.

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-2019-12948 8.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L)

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:

https://support.polycom.com/content/support/security-center.html For the latest information.

You might also find value in the high-level security guidance and security news located at:

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

Revision History

Revision 1.0 - Original publication: July 26th, 2019
Revision 1.1 – Modified page break: August 2nd, 2019
Revision 1.2 – Updated software version for UCS 4.1.1: December 20th, 2019

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 Poly has been advised of the possibility of such damages.