SECURITY ADVISORY – INFORMATION DISCLOSURE VULNERABILITY POLY VoIP PHONES

Advisory Version 1.0

DATE PUBLISHED: Feb 22, 2021

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

Please Note: 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 Poly VVX, CCX and Trio models running UC software could allow an authenticated, remote attacker to obtain sensitive device configuration information.

A successful exploit could allow the attacker to extract sensitive information from the affected device. The vulnerability is due to clear-text storage and weak permissions on the related file.

Solution

Poly has released firmware updates that address this vulnerability. There are no workarounds that address this this vulnerability. Please refer to the release notes for more information to confirm the supported hardware and software configurations are used.

Model	Firmware	Notes
VVX	UCS 6.1.2.1167 rev C , UCS 6.3.1.11465 rev M, UCS 5.9.6.2996 rev H, 6.2.1.1508	N/A
CCX and Trio	UCS 7.0.0.4332	N/A
CCX	UCS 6.2.23.0304	N/A
Trio	UCS 5.9.5.3153	N/A

CVSS v3 Base Metrics

To assist our customers in the evaluation of this vulnerability, Poly 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-# TBD) 5.8 Medium CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Poly Technical Support – either call 1-888-752-6876 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

Poly's Vulnerability Disclosure Policy can be found at:

https://support.polycom.com/content/dam/polycom-support/global/documentation/product-vulnerability-disclosure-policy.pdf

Revision History

Revision 1.0 - Original publication: Feb 22, 2021

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.