SECURITY ADVISORY – INFORMATION DISCLOSURE VULNERABILITY POLY VoIP PHONES

Advisory Version 1.0

DATE PUBLISHED: April 29th, 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

An information disclosure vulnerability exists in Poly CCX 400, 500, 600 and 700 and Trio 8500, 8800 and C60 models running UC software that could allow an authenticated administrative user to obtain sensitive information.

A successful exploit could allow the attacker to extract sensitive information from the affected device. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly.

Solution

Poly has released firmware updates that address this vulnerablity. 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	Vulnerable Firmware	Fixed Firmware Release
Trio 8800/8500	UCS 5.9.5 UCS 7.0.0 UCS 7.0.1	UCS 5.9.5.3182 UCS 7.0.1.1144
CCX	UCS 6.2.23 UCS 7.0.1	UCS 6.2.23.0387 UCS 7.0.1.1145
Trio C60	UCS 7.0.0 UCS 7.0.1	UCS 7.0.1.1143

Mitigation

Poly recommends all customers upgrade to the latest version. Customers who need time to upgrade may disable the Web User Interface (Web UI) either by changing settings in the phone's user interface or through configuration file changes. Please check your product's Administrator Guide for specific instructions on how to do this.

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 v3.1 Scores

(CVE-2021-TBA) 4.4 Meduim CVSS:3.1 = AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

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

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: April 29th, 2021

While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical errors, out of date information, or any errors or omissions in the content of this document. Poly reserves the right to change or update this document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical Bulletin.

Limitation of Liability
Poly 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 Poly 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 Poly has been advised of the possibility of such damages.