Vulnerability Summary

A vulnerability in the local user interface of the CCX500 phones could allow a local attacker access to restricted device settings. The vulnerability is due to a lack of restrictions on some device settings. A successful exploit could allow the local attacker to enable restricted options or change persistent system configuration settings.

Products Affected

The vulnerability affects the CCX500 with the software version 1.0.0.2535.

Solution

Poly has released a software update that addresses this vulnerability. There are no workarounds that address this vulnerability. CCX500 devices running software version 1.0.0.2535 should be updated to at least UCS_CCX_5.9.12.1111, which can be downloaded from the Poly Support website at:

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

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.
CVSS v3 Scores

The score provided is a representation of the base score to assist organizations with assessing risk for their environment, there is no published CVE related to this vulnerability.


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: January 22, 2020