SECURITY ADVISORY – Hard-coded credentials vulnerability in VVX products – Advisory Version 1.1

DATE PUBLISHED: June 17th, 2019

Any information in this Advisory is subject to change.

Please Note: This is a living document and may be subject to updates. The newest version of this document can be found at the following URL:

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

Vulnerability Summary

VVX products with software versions including and prior to, UCS 5.9.2 with Better Together over Ethernet Connector (BToE) application 3.9.1, use hard-coded credentials to establish connections between the host application and the device.

Products Affected

All VVX products with software versions including and prior to, UCS 5.9.2 with Better Together over Ethernet Connector (BToE) application 3.9.1, are susceptible to hard-coded credentials vulnerability.

Solution

Products	**Fix**
VVX300, VVX310, VVX400, VVX410, VVX500 and VVX600	Update UCS software to version 5.9.3 or later with compatible BToE Application
VVX201, VVX301, VVX311, VVX401, VVX411, VVX501 and VVX601 VVX150, VVX250, VVX350, VVX450.	Update UCS software to version 6.0.0 or later with compatible BToE Application

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

Note:

If any of the components are not upgraded to the above mentioned version then the communication will be done using SSH protocol. This is done to maintain a seamless upgrade during deployments, wherein the upgrade cycle for both the UCS and BToE connector application are different.

The support for SSH protocol will be permanently removed in the subsequent software release in both UCS and BToE connector application.

Recognition

We would like to thank the independent security researcher **Philipp Buchegger** from **SySS GmbH** for discovering this vulnerability, alerting us, and for his cooperative disclosure.

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-2019-10688 5.1 (AV:P/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L)

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:

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: April 23rd, 2019
Revision 1.1 - Fix version for multiple products: June 17th 2019