SECURITY ADVISORY – Hard-coded credentials vulnerability in VVX products – Advisory Version 1.0

DATE PUBLISHED: April 23rd, 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 using UCS software version 5.8.0 and earlier with Better Together over Ethernet Connector (BToE) application version 3.8.0 and earlier uses hard-coded credentials to establish connection between host application and device.

Products Affected

VVX products using UCS software version 5.8.0 and earlier with BToE application version 3.8.0 and earlier is vulnerable to hard-coded credentials vulnerability.

Solution

Update UCS software to version 6.0.0 or later with BToE App version 4.0.0 or later from the following URL:


https://downloads.polycom.com/voice/btoe/Polycom_BToE_Connector_4.0.0.0.zip

Note:

If any of the components is not upgraded to the above mentioned version then the communication will be done using SSH protocol. This has been done in order to maintain seamless upgrade in the deployments wherein the upgrade cycle for both UCS and BToE connector application is 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


For more information on CVSS v3 please see: https://www.first.org/cvss

Severity: Medium

<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.</td>
</tr>
<tr>
<td>High</td>
<td>A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.</td>
</tr>
<tr>
<td>Medium</td>
<td>A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.</td>
</tr>
<tr>
<td>Low</td>
<td>A vulnerability that has minimal impact to the system and is extremely difficult to exploit.</td>
</tr>
</tbody>
</table>

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