Security Advisory Relating to Vulnerabilities in Polycom VVX Phones and UC Software

DATE PUBLISHED: June 25, 2018

Any information in this advisory is subject to change.

Please note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this bulletin has been repaired against that vulnerability. The newest version of this document will always reside at the following URL:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Summary of Vulnerabilities

VVX phones running UC Software versions earlier than 5.8.0.12386 contain weaknesses associated with user passwords and their corresponding password hashing algorithms.

Solution

Update VVX to run UC Software version 5.8.0.12386 or later, which fixes these vulnerabilities.

Mitigations

Polycom recommends following standard best practices for Unified Communications, as detailed in our best practices paper found at:


Recognition

We would like to thank Brian Camp for disclosing this vulnerability to Polycom.
CVSS v3 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom leverages 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 Score:


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

Severity: High

<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:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

For the latest information. You might also find value in the high-level security guidance and security news located at:

http://www.polycom.com/security

Revision History

Revision 1.0 - Original publication: June 25, 2018