Security Advisory Relating to Vulnerabilities with UCS Software for Polycom VVX Phones

DATE PUBLISHED: July 3rd, 2018

This information applies to Polycom products and vulnerabilities discovered with the UCS software on the VVX phone lines, specifically VVX with UCS 5.7.0, UCS 5.7.1, UCS 5.7.2 and UCS 5.8.0. This advisory also applies to Hot Fixes based on affected software (example: UCS 5.7.1 B).

Any information in this advisory is subject to change as our investigation progresses.

Please Note: This is a living document, and Polycom will update this advisory regularly as the investigation progresses and new information becomes available. 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

Change Summary

In certain configurations, Polycom UCS Software for VVX Phones may disclose sensitive information.

Polycom has found that recent software releases for the VVX line of phones may potentially disclose sensitive information when using Web Proxy Auto Discovery (WPAD) in a Microsoft environment.

Impact and Risk

If the phone is configured to use web proxy but no web proxy credentials are provided, there is a risk that potentially disclose sensitive information. This vulnerability could allow a privileged, local attacker, in specific circumstances, to read sensitive information. To exploit this vulnerability, an attacker must be able to access the VVX management interface and successfully log into an affected device.

The following releases are potentially vulnerable and have been pulled from the Polycom Support website:

- UCS 5.7.0.11768
- UCS 5.7.1.2205
- UCS 5.7.2.1277
- UCS 5.8.0.12386

Additionally, all hotfixes released prior to June 21, 2018 based on affected software will be subject to this vulnerability. (Example: UCS 5.7.1 R) Should you be using an affected hot patch in a Microsoft environment, Polycom will contact you and provide you with a new build.

Polycom has released software updates that address this vulnerability. These updates can be found at:

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

Please select the model of your VVX phone and download the appropriate update.

Polycom is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Mitigations

Polycom recommends that customers download and install the updated version of our VVX software to avoid this vulnerability. Please consult the administrators guide for your phone model or contact Polycom support if you need assistance.

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:

UCS on VVX Vulnerabilities: 6.2 **High** (CVSS:3.0/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N)

For more information on CVSS v3 please see: https://nvd.nist.gov/vuln-metrics/cvss

Severity: High

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 change 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 may also find value in the security guidance and security news located at:

http://www.polycom.com/security

Note

The below applies to all Polycom security publications:

Polycom may at times issue either a ***Security Advisory*** or a ***Security Bulletin*** with regards to a particular vulnerability or set of vulnerabilities. If a ***Security Advisory*** is issued, this means that one more Polycom products are under investigation or verified by Polycom to be affected by one or more vulnerabilities. If a ***Security Bulletin*** is issued, Polycom is providing its customers with information about one or more vulnerabilities that have not been found by Polycom to directly affect any Polycom products, but that may be mistakenly thought to affect Polycom products. A ***Security Advisory*** might also be issued when a customer's environment might be affected, when false positives might occur from vulnerability scans, or when any other possible (but not actual) concern might exist regarding Polycom products and the vulnerability.

Revision History

Revision 1.0 – Original publication: June 25th, 2018
Revision 1.1 – Updates for fixed software version and mitigations: July 3rd, 2018