SECURITY ADVISORY – Vulnerabilities in Polycom QDX 6000 - Version 1.0

Security Advisory Relating to Cross Site Scripting (XSS) and Cross Site Request Forgery (CSRF) in QDX 6000

DATE PUBLISHED: March 2, 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

Vulnerability Summary

A stored cross site scripting (XSS) vulnerability has been discovered in the web application functionality of Polycom's QDX 6000 endpoint. This vulnerability could allow a remote attacker to execute arbitrary Javascript on QDX client users' web browsers.

In addition, a cross site request forgery (CSRF) vulnerability has been discovered in QDX's web application interface. If a user who is currently logged into the QDX were to point their browser to an attacker-controlled website that contains the CSRF attack, this vulnerability could allow the attacker to change arbitrary configuration settings on the QDX.

Solution

QDX 6000 is no longer supported by Polycom, and no code updates are planned for fixing these vulnerabilities. Instead, Polycom recommends applying the mitigations listed below or updating to a supported product such as Polycom Group Series endpoints.

Mitigations

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

http://support.polycom.com/global/documents/support/documentation/polycom_uc_security_best_practices_2015.pdf

In addition, Polycom recommends:

1. Enabling security mode: This can be done by going to the QDX web UI > admin settings > general settings > check the box for “security mode”, and then clicking on the “update” button.
2. Disabling web remote access: This can be done by going to the QDX web UI > admin settings > general settings > uncheck the box for “Web” under “Enable Remote Access”, and then clicking the “update” button.

Recognition

An independent security researcher, Bhaskar Borman (@BhaskarBorman on Twitter), alerted Polycom to these vulnerabilities. Polycom thanks Bhaskar for disclosing this vulnerability to us.

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:

7.6 – CVSS:3.0/AV:A/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N

For more information on CVSS v3 please see: https://www.first.org/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 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: March 2, 2018