



## 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](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](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
<b>Critical</b>	A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.
<b>High</b>	A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.

<b>Medium</b>	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
<b>Low</b>	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](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

---

©2018, Polycom, Inc. All rights reserved.

### Trademarks

POLYCOM®, the Polycom logo and all names and marks associated with Polycom and Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

### DISCLAIMER

WHILE POLYCOM USES REASONABLE EFFORTS TO INCLUDE ACCURATE AND UP-TO-DATE INFORMATION IN THIS DOCUMENT, POLYCOM MAKES NO WARRANTIES OR REPRESENTATIONS AS TO ITS ACCURACY. POLYCOM ASSUMES NO LIABILITY OR RESPONSIBILITY FOR ANY TYPOGRAPHICAL ERRORS, OUT OF DATE INFORMATION, OR ANY ERRORS OR OMISSIONS IN THE CONTENT OF THIS DOCUMENT. POLYCOM RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. INDIVIDUALS ARE SOLELY RESPONSIBLE FOR VERIFYING THAT THEY HAVE AND ARE USING THE MOST RECENT SECURITY ADVISORY OR SECURITY BULLETIN.

### LIMITATION OF LIABILITY

POLYCOM AND/OR ITS RESPECTIVE SUPPLIERS MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THIS DOCUMENT FOR ANY PURPOSE. INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND AND IS SUBJECT TO CHANGE WITHOUT NOTICE. THE ENTIRE RISK ARISING OUT OF ITS USE REMAINS WITH THE RECIPIENT. IN NO EVENT SHALL POLYCOM AND/OR ITS RESPECTIVE SUPPLIERS BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION), EVEN IF POLYCOM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

