SECURITY ADVISORY 112490
Advisory Version 2.0

Advisory Relating to Multiple Cross-site Scripting (XSS) Vulnerabilities in Polycom® HDX® Video Endpoints.

DATE PUBLISHED: September 16th, 2016

This information applies to all models of Polycom HDX video endpoints running HDX system software versions:	3.1.9 and earlier

Please Note: This is a living document, and will be updated as necessary. 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

Polycom HDX video endpoints (all models) are subject to multiple cross-site Scripting (XSS) vulnerabilities that could be maliciously abused to gain unauthenticated access to the camera or execute JavaScript in the context of pages viewed by administrators.

Details

The web interface of HDX endpoints is subject to persistent unauthenticated cross-site scripting using a crafted username with an incoming call, which may allow malicious users to access or control the camera.

A malicious user with administrative privileges can submit diagnostic content that contains embedded JavaScript. Stored XSS occurs when a web application gathers input from a user, and then stores that input for others to potentially retrieve and view. Any administrator who subsequently views the malicious submission will execute the JavaScript in the context of their web browser.

Polycom has implemented changes to the HDX system software to address these XSS vulnerabilities in versions starting with 3.1.10.

HDX administrators can download a non-vulnerable HDX system software version through this link:
http://support.polycom.com/PolycomService/support/us/support/video/hdx_series/

Any customer using an affected endpoint who is concerned about this vulnerability within their deployment should contact Polycom Technical Support— either call 1-800-POLYCOM or log a ticket online at:

http://support.polycom.com/PolycomService/home/home.htm

Mitigations

For customers who cannot immediately upgrade to a non-vulnerable HDX system software version, the most effect means to mitigate these vulnerabilities is to limit access to the web interface of the HDX to only trusted users, and to limit sources of incoming calls to trusted remote endpoints.

The vulnerable field for the stored XSS is only accessible to HDX administrators via the web. This vulnerability is not triggered through the HDX console, only through the web interface.

In addition, we recommend administrators follow standard best practices and change all default passwords and restrict network web access to the HDX unit using firewalls and whitelists.

CVSS v2 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 v2 Scores:

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) – persistent unauthenticated XSS
5.2 (AV:A/AC:L/Au:S/C:P/I:P/A:P) – stored XSS

For more information on CVSS v2 please see:
http://www.first.org/cvss/cvss-guide.html

Severity: Medium

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.

Acknowledgements

The persistent unauthenticated XSS was first discovered and brought to Polycom’s attention by an anonymous security researcher working with Beyond Security's SecuriTeam Secure Disclosure program. The stored XSS vulnerability was first discovered and brought to Polycom’s attention by Vincent Hutsebaut of NCIRC. We would like to thank Beyond Security, Mr. Hutsebaut and NCIRC for their coordinated disclosure of these vulnerabilities.

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 29, 2016 – First Announcement
Revision 2.0 – Second publication: September 16, 2016 – Additional Details / Acknowledgement

Trademarks

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 Technical Advisory.

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.