SECURITY ADVISORY: Multiple vulnerabilities in HDX products – Advisory Version 1.0

DATE PUBLISHED: April 26th, 2019

Any information in this Advisory is subject to change.

Please Note: This is a living document and may be subject to updates. The newest version of this document can be found at the following URL:

https://support.polycom.com/content/support/security-center.html

Vulnerability Summary

Four security vulnerabilities in HDX Series products have been fixed in release 3.1.14.

a. **CVE-2019-11355** : The CSR generation tool is subject to Remote Code Execution. Administrators logged in to the web UI can abuse this to attain privileged access to the operating system.

b. A stored XSS defect in the closed caption utility allows anyone who can login to the HDX web UI to potentially run malicious javascript on other web UI clients who view the closed caption output.

c. The deployed embedded web server in Polycom HDX systems allows HTTP Verb Tampering. The server fails to validate the HTTP requests to specific verbs. It is possible to disclose system information by tampering the HTTP verb (*e.g.* changing HTTP POST to HTTP GET).

d. The Remote Access component fails to validate input passed by a user of the web UI, and is thus vulnerable to XSS exploitation that can execute javascript payloads in the context of the user.

Products Affected

HDX products using software version 3.1.13 and earlier are vulnerable to the four issues in the summary.

Solution

Update HDX software to version 3.1.14 or later for your specific model from the following URL:

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

Recognition

We would like to thank **WootCloud** (https://www.wootcloud.com) for discovering the two XSS and the Verb Tampering vulnerabilies, alerting us, and for their cooperative disclosure.

We would like to thank **Hyunjin Ko** for his discovering, reporting, and cooperative disclosure on the RCE vulnerability in the CSR generation tool (CVE-2019-11355).

CVSS v3 Base Metrics

To assist our customers in the evaluation of this vulnerability; Poly uses 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 Scores

a.	RCE in CSR generation tool	**9.1** (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
b.	Stored XSS in closed captions	**3.5** (AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N)
c.	HTTP Verb Tampering	**4.3** (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
d.	XSS in Remote Access component	**3.5** (AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/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 Poly Technical Support – either call 1-800-POLYCOM or visit:

https://support.polycom.com/content/support/security-center.html

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

https://support.polycom.com/content/support/security-center.html

Revision History

Revision 1.0 - Original publication: Apr 26, 2019

Trademarks

Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. 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 Poly.

Disclaimer

While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical errors, out of date information, or any errors or omissions in the content of this document. Poly 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 Bulletin.

Limitation of Liability

Poly 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 Poly 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 Poly has been advised of the possibility of such damages.