Security Advisory Relating to Remote Code Execution Vulnerability on Polycom HDX Endpoints

DATE PUBLISHED: November 24, 2017

Any information in this advisory is subject to change.

Please note: 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 critical vulnerability has been discovered in the Polycom shell (psh) functionality on the HDX's diagnostics port (port tcp/23). This vulnerability could allow a remote attacker to execute arbitrary code on the HDX, which could lead to compromise of the system.

Products Affected

HDX 3.1.11 hotfix 1 and earlier	Fixed in HDX 3.1.11 hotfix 2 or later

Solution

Update to HDX Version 3.1.12 Software or later, available at the Polycom Support web site:

http://support.polycom.com/content/support/North_America/USA/en/support/video/hdx_series.html

You can mitigate the vulnerability by following the mitigations listed below.

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

As detailed in our best practices paper, Polycom specifically recommends that endpoints such as HDX be placed behind a firewall and not be directly accessible from the Internet.

In addition, Polycom recommends enabling HDX's "Secure Mode" by logging into the web UI > Admin Settings > Security > Security Settings and checking the box for "Secure Mode". This will require users to authenticate before they can access the HDX's diagnostics port.

Once the admin checks the box for Secure Mode they are prompted to enter a "room password" for the HDX. Polycom recommends making the password at least 12 characters long, using upper and lower case and special characters, and not containing easily-guessable strings like "polycom" or "password".

Recognition

Polycom appreciates and values the members of the security research community who find vulnerabilities, bring them to our attention, and work with Polycom in a coordinated effort so that security fixes can be issued to all impacted customers. We would like to thank the independent security researchers at SensePost for discovering this vulnerability and alerting 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:

8.0 - CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

For more information on CVSS v3 please see: https://www.first.org/cvss

Severity: Critical

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment or has questions about the solution or mitigation recommendations described above should contact Polycom Technical Support by calling 1-800-POLYCOM or visiting:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

You might also find value in the latest high-level security guidance and security news from Polycom, which is located at:

http://www.polycom.com/security

Revision History

Revision 1.0 - Original publication: November 15, 2017
Revision 1.1 – Updated publication with Hotfix availability: November 15, 2017
Revision 1.2 – Updated publication with GA build availability: November 24, 2017

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.