



SECURITY BULLETIN – HDX versions older than 3.1.13 can be affected by multiple Botnets - Version 1.0

Security Bulletin Related to HDX (versions older than 3.1.13) can be affected by multiple Botnets

DATE PUBLISHED: February 20, 2019

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:

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

Summary

Polycom HDX endpoints that are running software versions older than 3.1.13 contain security vulnerabilities that have been previously listed on the Polycom Security Center (see link above). These security vulnerabilities may render HDX endpoints vulnerable to takeover by a botnet.

A botnet is a network of computer systems that have been infected with malicious software and controlled as a group without the systems owners' knowledge. Currently Polycom HDX endpoints can be affected by Yowai, Hades and Bushido Botnets.

Solution

Update HDX endpoints to software version 3.1.13, which fixes known vulnerabilities and protects against botnets and other infections. You can download version 3.1.13 from:

<https://support.polycom.com/content/support/north-america/usa/en/support/video/hdx-series.html>

To determine if an HDX is infected with a botnet, or has been exploited by known vulnerabilities in older versions of HDX software, perform the following steps:

- Login to the HDX web UI
- Go to the "diagnostics" tab
- Click on "download logs"
- Click on "download support information package"

- Your browser will download a file named “polycom_info...tgz”.
- Uncompress this file, this will result in several files whose names start with “messages”
- Examine these files for the occurrence of this string: \${IFS} (without spaces)

If \${IFS} appears in any log files, the HDX has been exploited by a known vulnerability in old HDX software, and the HDX should be factory reset and updated to 3.1.13 as soon as possible.

Mitigations

Polycom recommends keeping the HDX endpoint’s software up-to-date.

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

<https://support.polycom.com/content/dam/polycom-support/global/documentation/polycom-uc-security-best-practices-2015.pdf>

Recognition

We would like to thank WootCloud (<https://www.wootcloud.com>) for discovering the threat, alerting us, and for their cooperative disclosure.

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:

<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: February 20, 2019

SECURITY BULLETIN – HDX ENDPOINTS (VERSIONS OLDER THAN 3.1.13) CAN BE AFFECTED BY MULTIPLE BOTNETS - VERSION 1.0

©2019, 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.

