

Security Bulletin 107522

Security Advisory Relating to the Firmware Update Command Injection Vulnerability on Polycom® HDX® Video Endpoints

This information applies to Polycom HDX Video Endpoints running software versions:

Commercial 3.0.5

Description

The Polycom HDX is susceptible a command injection vulnerability which allows an authenticated malicious user to execute arbitrary commands on the system when using the firmware update functionality.

Status

Polycom made changes to the HDX systems starting with the commercial software build 3.1.1.2 to prevent this vulnerability. Input validation was improved so that commands are no longer processed as instructions and the software update will be aborted.

HDX Administrators can download commercial version 3.1.1.2 or newer at the link provided below to avoid this potential problem.

http://support.polycom.com/PolycomService/support/us/support/video/hdx_series/index.html

There are several workarounds that can be applied to limit or negate this vulnerability until the fixed release can be certified. Please see the Mitigation section below.

Any customer using one of the affected products that 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>

Mitigation

For customers who cannot upgrade to a fixed version, administrators can:

- Disable the web interface on the HDX,
- Use the Whitelist option to limit connections to the web management interface to certain, approved IP addresses.

Please consult the HDX Administrator's Guide for information and instructions on these options.

Revision History

Revision 1.0 – March 13, 2013 - Initial Release.

Acknowledgement

This vulnerability was discovered and brought to Polycom's attention by Moritz Jodeit of n.runs. We thank Mr. Jodeit and n.runs for their responsible disclosure of this vulnerability.

Trademark Information

© 2013, Polycom, Inc. All rights reserved. Polycom®, the Polycom logo design, and the names and marks associated with 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 the 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.