Security Bulletin 107526

Security Advisory Relating to the PUP File Header MAC Signature Bypass on Polycom® HDX® Video Endpoints

This information applies to Polycom HDX Video Endpoints running software versions:	Commercial 3.0.5 and earlier

Description

The Polycom HDX uses a software update process that reads in a PUP file containing all of the information and tools needed to properly update the system. A vulnerability has been discovered in the PUP file header MAC signature verification process allowing a malicious user to extract the components of the PUP file.

Status

Polycom made changes to the HDX software starting with the commercial software build 3.1.1.2 to prevent this vulnerability. The software update process was changed to remove the utilities that would allow a malicious user to potential modify the PUP file. The HDX PUP file also uses a public key DSA signature to protect the integrity of the file; this additional layer of protection is not compromised by this vulnerability. While users may not notice any change within the user interface, the update process has been improved to address potential security problems.

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

Only upgrade HDX systems using PUP files obtained from Polycom.

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.

Revision History

Revision 1.0 – March 13, 2013 - Initial Release.

Trademark Information