Security Bulletin 107524

Security Advisory Relating to the H.323 Format String 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 to a format string vulnerability via a maliciously crafted call setup message that could lead to systems instability or remote code execution.

Status

Polycom made changes to the HDX software starting with the commercial software build 3.1.1.2 to prevent this vulnerability. Input validation was improved so that these special characters are no longer allowed in systems names and are also no longer processed as instructions.

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, Polycom recommends that customers evaluate network access control lists, firewalls and other network protection to ensure that they have been deployed in a manner that is consistent with security best practices. The risk presented by this potential vulnerability to Polycom products, as well as other networked devices, may be mitigated by these controls. Customers should also ensure that Polycom products have been configured as recommended by Polycom implementation guides.

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