Security Bulletin 101521

Security Advisory Relating to Deloitte Advisory #DTTAR-20120001 on Polycom® HDX® Video End Points

This information applies to Polycom HDX Video End Points running software versions:	Commercial 3.0.4
	UC APL 2.7.1_J

Symptom

The web management interface on affected versions of the HDX is vulnerable to cross-site scripting. This vulnerability could be exploited allowing malicious scripts to be inserted and executed on the HDXs web interface, potentially destabilizing the system or introducing security risks to users of the system.

Cause

The web management interface failed to adequately sanitize input in certain input fields. When specially crafted URLs were called, the attacker's scripts will execute.

Status

Polycom made changes to the HDX systems starting with the commercial software build 3.0.5 to prevent this vulnerability. A fixed build of the UC APL version will be going through certification testing shortly and will be available as 2.7.1.1_J.

HDX Administrators can download commercial version 3.0.5 or newer at the link provided below to avoid this potential problem.

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

There is not a certified build for customers who require the UC APL version at this time. However, Polycom has posted a fixed build of 2.7.1.1_J on our Government Certification and Accreditation website that will be going through certification testing shortly. The build is available at:

http://www.polycom.com/solutions/solutions-by-industry/us-federal-government/certification-accreditation.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 Workaround 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 .

Workaround

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

- Disable the option for web management on HDX,

- Put the HDX unit into Maximum Security Mode. This will require the loading and use of PKI certificates, to establish mutual TLS sessions between the HDX and any users of the Web interface, and/or

- 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.

This information applies to Polycom HDX Video End Points running software versions:	Commercial 3.0.4
	UC APL 2.7.1_J

Acknowledgement

This vulnerability was discovered and brought to Polycom's attention by Fara Rustein (@fararustein) of Deloitte Argentina. We thank Ms. Rustein and Deloitte Argentina for their responsible disclosure of this vulnerability.

Trademark Information