# Advisory Relating to an XML External Entity (XXE) Vulnerability in Polycom® HDX® Video Endpoints.

DATE PUBLISHED: June 29th, 2016

| | |
|---|---|
| This information applies to all models of Polycom HDX video endpoints running HDX system software versions: | 3.1.9 and earlier |

*Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this advisory has been repaired against that vulnerability. The newest version of this document will always reside at the following URL:*

*http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html*

## Vulnerability Summary

Polycom HDX video endpoints (all models) are vulnerable to XML External Entity (XXE) manipulations, which could be used by a malicious party to deny service to the web interface of the HDX system.

## Details

This XXE vulnerability exploits a capability in XML DTDs (Document Type Definitions) that allows the creation of custom macros or entities. By recursively defining custom entities at the top of a document, an attacker can overwhelm the XML parser, preventing legitimate web traffic from being processed.

Polycom has implemented changes to the HDX system software to address these XSS vulnerabilities in versions starting with 3.1.10.

HDX administrators can download a non-vulnerable HDX system software version through this link: http://support.polycom.com/PolycomService/support/us/support/video/hdx_series/

Any customer using an affected endpoint who 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**

## Mitigations

For customers who cannot immediately upgrade to a non-vulnerable HDX system software version, the most effect means to mitigate this vulnerability is to limit access to the web interface of the HDX to only trusted users. The vulnerable component is only accessible to HDX administrators via the web.

The HDX console does not suffer from lack of responsiveness similar to the web interface, so system recovery is possible through the console interface.

In addition, we recommend administrators follow standard best practices and change all default passwords and restrict network web access to the HDX unit using firewalls and whitelists.

## CVSS v2 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom leverages the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v2 Scores:

2.7 (AV:A/AC:L/Au:S/C:N/I:N/A:P)

For more information on CVSS v2 please see:
http://www.first.org/cvss/cvss-guide.html

## Severity: Medium

| Rating | Definition |
|--------|------------|
| Critical | A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware. |
| High | A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources. |
| Medium | A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit. |
| Low | A vulnerability that has minimal impact to the system and is extremely difficult to exploit. |

## Acknowledgement

This vulnerability was first discovered and brought to Polycom's attention by Vincent Hutsebaut of NCIRC. We would like to thank Mr. Hutsebaut and NCIRC for their coordinated disclosure of these vulnerabilities.

## 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:*

*http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html*

*For the latest information. You might also find value in the high-level security guidance and security news located at:*

*http://www.polycom.com/security*

## Revision History

Revision 1.0 - Original publication: June 29th, 2016 – First Announcement