SECURITY ADVISORY 9611
Advisory Version 1.0 – Initial Release

Advisory Relating to Polycom® RealPresence® Capture Server and RealPresence® Media Suite Appliance Editions

DATE PUBLISHED: December 16th, 2015

This information applies to Polycom RealPresence Capture Server and RealPresence Media Suite Appliance Edition running versions:	2.0 and earlier 1.8 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

Appliance Edition models of Polycom RealPresence Capture Server and RealPresence Media Suite were delivered with a default configuration that exposed an IPMI administrative web interface with default credentials, when deployed on a network with DHCP.

Details

Polycom has implemented changes to the default configuration of RealPresence Media Suite to address these issues. Media Suite administrators can download system updates through this link:

http://support.polycom.com/PolycomService/support/us/support/network/video_content_management_solutions/realpresence_media_suite.html

The Baseboard Management Controller (BMC) on appliance edition hardware supports the Intelligent Platform Management Interface (IPMI). As shipped, the IPMI was configured to share the LAN 1 port but used a separate MAC address unique from the system.

On networks with DHCP service, this shared IPMI port was default configured to make a DHCP request and claim a unique network address. The IPMI subsystem would run a webserver that provided administrator-level access using default credentials to a variety of system configuration options.

Fix

RealPresence Media Suite version 2.1 disables shared networking of the IPMI web interface and customers are strongly encouraged to upgrade as soon as practical for their environment.

Mitigations

For customers who cannot upgrade to RealPresence Media Suite version 2.1 or newer, this issue will be mitigated in environments without a DHCP server on the same subnet as the appliance.

In network environments where DHCP is necessary, we recommend implementing either a whitelist or a blacklist on the DHCP server to disallow the IPMI system from claiming an address. In addition, we recommend administrators follow standard best practices and always restrict network access to the management interface of the appliance.

In environments with DHCP enabled, the network address of the webserver running on the IPMI port can be detected by closely observing the startup routine of the appliance console, or by using a network scan, sniffing the network for DHCP requests, or by monitoring the logs of the DHCP server.

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:

6.9 (AV:A/AC:M/Au:N/C: P/I: P/A:C)

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.

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: December 16th, 2015 – First Announcement