SECURITY ADVISORY 27896
Advisory Version 1.0 – Initial Release

Advisory Regarding Unauthorized SSH Tunnel Spam from Polycom® RealPresence® Group Series Video Endpoints and Resource Manager Systems.

DATE PUBLISHED: November 15th, 2016

The following Polycom products are affected:	
All models of Group Series video endpoints running system software versions:	4.3.0 -to- 5.1.2 (inclusive)
All editions of Resource Manager running system software versions:	8.4.1 (and earlier)

This document may be updated. The latest version will always reside at the following URL:
http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Vulnerability Summary

In certain configurations, unauthorized SMTP traffic may be relayed through an SSH tunnel and appear to have originated from a Polycom Group Series video endpoint or Resource Manager system. No other Polycom products have been found to be vulnerable.

Details

SSH was configured on these two products to allow TCP forwarding. Resource Manager uses network port 22 (SSH) for maintenance and support. Group Series video endpoints use this port for API communication with integrated devices such as Polycom Touch Control and RealPresence Touch.

Resource Manager was exploited through the PlcmSpIp provisioning account's documented password; Group Series endpoints were vulnerable through root password guessing. On neither product were these accounts accessible to a remote shell, due to configuration mitigations that were already in place.

Polycom has implemented changes to Resource Manager software to address these SSH Tunnel vulnerabilities starting with version 9.0 and to Group Series system software starting with version 6.0.

Group Series administrators can find documentation and download system software through this link:
http://support.polycom.com/PolycomService/support/us/support/video/group_series/

Resource Manager administrators can find documentation and system software through this link:
http://support.polycom.com/PolycomService/support/us/support/network/management_scheduling/realpresence_resource_manager.html

Mitigations

The most effective means to mitigate this vulnerability is to restrict access to the administrative address of any Polycom device to only trusted networks using firewalls and network segregation.

Disabling (or firewalling) port 22 on Group Series or Resource Manager also mitigates the problem.

With version 9.0, Resource Manager disables port 22 by default. In earlier releases, this can be disabled in the web interface through the “Disable Root User Login” checkbox, which may have been labelled “Allow Linux Console Access” or “Enable Remote Access Connections” in earlier releases.

Since 4.3.0, Group Series endpoints have offered administrators the option to disable SSH through the security settings in the web interface (“Enable SSH Access”) or via an API session (“sshenable false”).

We also recommend customers change default passwords and set complex administrator passwords.

CVSS 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 Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

Base CVSS v3 Score: 4.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

For more information on CVSS v2 and v3 please see:
https://www.first.org/cvss/v2/guide
https://www.first.org/cvss/specification-document

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

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: November 15th, 2016