Security Advisory Related to Cyber Threats Targeting Well-Known Default Passwords

DATE PUBLISHED: January 24th, 2019

This information is provided for increased awareness to the persistent cyber threats targeting well-known and documented default passwords and PINS used in network attached devices. Along with many other types of network attached devices, these threats are targeting unified communications devices that have been deployed in an insecure manner where manufacturer provided default passwords or PINs have not been changed.

Please Note: This is a living document, and Polycom will update this document in the event that new information becomes available. 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

Summary

Polycom is aware of persistent cyber threats targeting unified communications devices that have been deployed in an insecure manor where manufacturer provided default passwords or PINs have not been changed.

Cyber actors are scanning the internet for devices that are deployed, using default passwords and PINs. The malicious actors are attempting to gain unauthorized access to these devices to retrieve device and customer specific configuration information. This information may then be used to:

1. Gain intelligence related to the network configuration of the environment where the device is deployed; and,
2. Placing fraudulent international phone calls; or,
3. Identify devices that are running outdated firmware that may contain vulnerabilities, allowing the cyber actor to leverage targeted attacks against the vulnerable device.

Recommendations

Customers are encouraged to follow recommended best security practices:

1. Ensure that all default passwords have been changed; and,
2. Monitor and review logs to identify unusual activity, including failed login attempts; and,

3. Regularly patch and update systems and device firmware, these updates may include fixes that address vulnerabilities; and,
4. Disable unnecessary or unused services; and,
5. Configure firewalls and other network protection services to block traffic from unauthorized IP addresses; and,
6. Periodically change passwords and use a strong password; and,
7. Follow manufacture recommended best practices for a secure deployment.

Contact

For the latest information, you may also find value in the security guidance and security news located at:

http://www.polycom.com/security

Note

The below applies to all Polycom security publications:

Polycom may at times issue either a ***Security Advisory*** or a ***Security Bulletin*** with regards to a particular vulnerability or set of vulnerabilities. If a ***Security Advisory*** is issued, this means that one more Polycom products are under investigation or verified by Polycom to be affected by one or more vulnerabilities. If a ***Security Bulletin*** is issued, Polycom is providing its customers with information about one or more vulnerabilities that have not been found by Polycom to directly affect any Polycom products, but that may be mistakenly thought to affect Polycom products. A ***Security Advisory*** might also be issued when a customer's environment might be affected, when false positives might occur from vulnerability scans, or when any other possible (but not actual) concern might exist regarding Polycom products and the vulnerability.

Revision History

Revision 1.0 – Original publication: January 18th, 2019
Revision 1.1 – Slight revision to grammar for readability: January 24th, 2019

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.