SECURITY BULLETIN – Increased SIP Provisioning Attacks

Advisory Version 1.1

DATE PUBLISHED: February 24th, 2021

ANY INFORMATION IN THIS BULLETIN IS SUBJECT TO CHANGE.

Please Note: This is a living document and may be subject to updates. The latest version of this document can be found at the following URL:

https://support.polycom.com/content/support/security-center.html

Security Bulletin Relating to Increased SIP Provisioning Attacks

Poly 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 Poly or Polycom products are verified by Poly to be affected by one or more vulnerabilities.

If a **Security Bulletin** is issued, Poly is providing its customers with information about one or more vulnerabilities that have not been found by Poly to directly affect any of our products, but that may be mistakenly thought to affect our products. A Security Bulletin 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 Poly or Polycom products and the vulnerability.

Situation Summary

Poly along with several ITSPs have detected an increase in the number of attacks and reconnaissance efforts against VoIP provisioning services.

Situation Details

Attackers are programmatically attacking provisioning services utilizing different vectors attempting to exploit potential weaknesses in the provisioning service to extract service provider provisioning information. In some attacks, the attackers are impersonating legitimate VoIP devices. When successful, the attackers may use this information to commit toll-fraud, caller ID spoofing and SPAM over Internet Telephony (SPIT), launch Denial of Service (DoS) attacks or use the information gathered in other fraudulent VoIP activities.

Impact and Risk

Since the attack is so widespread, its purpose cannot be truly uncovered. Each target network is different both in purpose and in layout, no one statement can be made about impact and risk.

Attackers are likely looking for a means to conduct toll fraud – dialing calls through third-party systems, without the consent of the owners of those third-party systems and examine device capabilities and gather information on potential targets.

General Mitigations

One of the best protections against the type of attack is to implement subscriber device authentication using a combination of MAC address authentication and digital certificate Common Name Validation. While this cannot prevent a specific compromised phone from obtaining credentials, it does help prevent an attack vector that uses a single compromised device to attempt to extract information for multiple phones.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Poly Technical Support – either call 1-888-752-6876 or visit:

https://support.polycom.com/content/support/security-center.html for the latest information.

Poly's Vulnerability Disclosure Policy can be found at:

https://support.polycom.com/content/dam/polycom-support/global/documentation/product-vulnerability-disclosure-policy.pdf

Revision History

Revision 1.0 - Original publication: Feb 22, 2021
Revision 1.1 – typographical corrections: Feb 24, 2021

While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical errors, out of date information, or any errors or omissions in the content of this document. Poly reserves the right to change or update this document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical Bulletin.

Limitation of Liability
Poly 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 Poly 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 Poly has been advised of the possibility of such damages.