SECURITY BULLETIN – Cybersecurity and Infrastructure Security Agency (CISA) Alert AA20-352A

Advisory Version 1.0

DATE PUBLISHED: January 20th, 2021

ANY INFORMATION IN THIS ADVISORY 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

Summary

In response to the Cybersecurity and Infrastructure Security Agency (CISA) alert AA20-352A, Plantronics, Inc. (“Poly”) launched an investigation to determine if any Poly systems were vulnerable. Poly verified an instance of the vulnerable SolarWinds Orion product running in the Poly environment. The systems running the vulnerable software were immediately shut down and disconnected from the network.

Following the guidance provided by SolarWinds and the U. S. Department of Homeland Security (DHS), the Poly Security Office and IT teams moved quickly to address the issue. The vulnerable software was patched, and related systems have been rebuilt.

The teams reviewed audit logs and other security systems for Domain indicators of compromise IOCs, Hashes, Threat Triggers and EUBA for other IOCs documented for this vulnerability. These investigations did not uncover any signs of malicious activity or indicators of compromise and there are no other indications that machines used by Poly were targeted.

Solution

There is no known impact to Poly products or services we provided to our customers. Poly will continue to investigate and monitor Poly systems and technologies for any anomalous behavior related to this incident.

For more information, please see the write up on the CISA website here:

https://us-cert.cisa.gov/ncas/alerts/aa20-352a

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:

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

You might also find value in the high-level security guidance and security news located at:

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

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: January 20th, 2021