SECURITY ADVISORY– Plantronics Hub – CVE-2020-14941 Local Privilege Escalation

DATE PUBLISHED: June 10, 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

Vulnerabilty Summary

A vulnerability in the Plantronics Hub updater system, if exploited, could allow an authenticated local attacker, to execute arbitrary code on an affected device as the Microsoft Windows SYSTEM account.

The vulnerability is due to overly broad signature acceptance for Poly signed binaries. An attacker could exploit this vulnerability by executing commands or binaries with SYSTEM privileges.

Products Affected

Plantronics Hub versions 3.21 and lower are affected.

Solution

Update to the lastest version of Plantronics Hub (3.22 or greater).

https://www.poly.com/us/en/support/downloads-apps/hub-desktop

Recognition

Polycom appreciates and values the members of the security research community who find vulnerabilities, bring them to our attention, and work with Polycom in a coordinated effort so that security fixes can be issued to all impacted customers. We would like to thank the independent security researcher **Giuseppe** from **Redtimmy** for discovering this vulnerability, alerting us, and for cooperative disclosure.

CVSS v3 Base Metrics

To assist our customers in the evaluation of this vulnerability,Poly uses 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

CVSS v3 Scores

The score provided is a representation of the base score to assist organizaitons with assessing risk for their environment, there is no published CVE related to this particular vulnerability.

CVSS Score: 8.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

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

Revision History

Release 1.0 – Original publication: 06/10/21