



## 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>

### Vulnerability 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 latest 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 organizations 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

---

©2020 Plantronics, Inc. All rights reserved.

### Trademarks

Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Poly.

### Disclaimer

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.

