



SECURITY BULLETIN – CX5100/ CX5500 – Authenticated Command Injection

DATE PUBLISHED: September 7, 2021

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

Please Note: Poly takes the security of our customers and our products seriously. 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 command injection flaw exists through an authenticated Telnet connection. A successful exploit of this vulnerability could allow the attacker to establish a shell with elevated privileges.

Products Affected

Product	Firmware	Fix
CX5100	1.3.5	End of Support June 30, 2021
CX5500	1.3.5	End of Support August 31, 2021

Mitigations

Poly recommends the applying the following methods to reduce the risk of the identified vulnerability. If possible, it is recommended to disable the web UI, which can be accomplished on the device using the Admin credentials for the device. It is also recommended to implement strong password complexity for the Admin account credentials.

Solution

Poly will not release a firmware update to resolve this issue as the device is at the end of the support window.

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 9.1

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

Recognition

Poly would like to thank **Caleb Jaren** and **Brendan Saunders** from Microsoft for reporting security vulnerabilities to us and for their coordinated disclosure.

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: September 7, 2021

©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.