SECURITY ADVISORY – KNOB AND BIAS BLUETOOTH VULNERABILITES AND POLY HEADSETS

Advisory Version 1.0

DATE PUBLISHED: July 21st, 2020

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

Two recent vulnerabilities have been identified in some Bluetooth enabled products. They are:

BIAS (CVE-2020-10135), a vulnerability in secure connection pairing in Bluetooth BR/EDR Core Specification v.5.2 and earlier which may allow an unauthenticated user to complete authentication without proper pairing credentials.

KNOB (CVE-2019-9506), a vulnerability in the Bluetooth BR/EDR Specification v.5.1 and earlier which is more succeptible to brute-force attacks potentially allowing traffic to be decrptyed.

Solution

Poly has released firmware updates that contain fixes for these issues as well as other fixes and features. These can be installed via the Plantronics Hub software. Please refer to the release notes for more information.

Model	Version	Notes
Calisto 3200/5300	v66	Includes fix for BIAS and KNOB vulnerabilities
BT600	v1723	Includes fix for BIAS and KNOB vulnerabilities
Voyager 4200 UC Series	v520	Includes fix for BIAS and KNOB vulnerabilities

Voyager 4200 Office Series	v323	Includes fix for BIAS and KNOB vulnerabilities
Voyager 4245 Office	v77	Includes fix for BIAS and KNOB vulnerabilities
Voyager 5200 UC	v508	Includes fix for BIAS and KNOB vulnerabilities
Voyager 5200 Office	v323	Includes fix for BIAS and KNOB vulnerabilities
Voyager 6200 UC	v706	Includes fix for BIAS and KNOB vulnerabilities
Voyager 8200 UC	v667	Includes fix for BIAS and KNOB vulnerabilities
Voyager Focus UC	v500	Includes fix for BIAS and KNOB vulnerabilities
Voyager Legend UC	v110	Includes fix for BIAS and KNOB vulnerabilities

The Plantronics Hub software, release notes, and other documentation for your Poly and Plantronics headsets can be found at:

https://www.poly.com/pl/pl/support/downloads-apps

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.

Base CVSS v3 Scores

BIAS (CVE-2020-10135)	5.4 MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
KNOB (CVE-2019-9506)	8.1 HIGH	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

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: July 21st, 2020

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.