



Security Incident Bulletin

KNOB and BIAS Bluetooth[®] vulnerabilities

Version 2.0 | 22 April 2021

Please note: This is a living document and may be subject to updates. The latest version can be found at www.jabra.com/support

Incident Summary

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

- **BIAS (CVE-2020-10135)** Legacy pairing and secure-connections pairing authentication in Bluetooth BR/EDR Core Specification v5.2 and earlier may allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. This authentication does not give the encryption key, but in combination with the below KNOB incident, it can allow brute-force attacks outside the pairing process.
- **KNOB (CVE-2019-9506)**, the Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka “KNOB”) that can decrypt traffic and inject arbitrary ciphertext without the victim noticing.

Incident Severity (CVSS)

CVSS v3 Base Metrics

In order to assess the Incident, we are using the CVSS v3 (Common Vulnerability Scoring System). CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. For more information regarding CVSS please see: <https://nvd.nist.gov/vuln-metrics/cvss>

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

Incident Solution

The following firmware updates include fixes for the BIAS and KNOB vulnerabilities. We strongly advise you to upgrade to these versions or later using the normal firmware update channels (Jabra Direct, Jabra Xpress, Jabra Sound+). For more information on firmware updates, refer to the product support page.

JABRA PRODUCT	FIXED IN THE FIRMWARE VERSION (A NEWER VER. MIGHT BE AVAILABLE)	FIX DESCRIPTION
Jabra Link 370	1.48.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Link 360	2.47	Includes fix for BIAS and KNOB vulnerabilities
Jabra Evolve 65	2.72.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Evolve 75	2.10.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Evolve 65e	2.22.2	Includes fix for BIAS and KNOB vulnerabilities
Jabra Evolve 75e	2.25.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Evolve 65t	2.34.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Speak 510	2.31	Includes fix for BIAS and KNOB vulnerabilities
Jabra Speak 710	1.38.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Speak 810	1.9.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite 65t	2.34.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite Active 65t	2.34.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite Active 45e	2.21.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite 45e	1.27.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite 65e	2.25.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite 85h	1.5.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Elite Sport	5.6.0	Includes fix for BIAS and KNOB vulnerabilities
Jabra Biz 2400 II USB BT	1.14	Includes fix for BIAS and KNOB vulnerabilities
Jabra Engage 65/75	4.2.0	Includes fix for BIAS and KNOB vulnerabilities

All new products launched after October 31, 2019 should not be impacted by this security incident.

Support

If you have questions about the incident described in this bulletin, please email security-center@jabra.com