Information note

Topic **Security Advisory for Bluetooth BLUFFS Vulnerability (CVE-2023-24023)**
UBXDOC-132308279-35907 C1-Public

Author Martin Furmanski

Date 26 July 2024

1 Affected products

The following u-blox products are affected.

Product name	Variants	Remarks
OBS421	All	Uses a minimum key length of 5 octets since it's an older generation product. We recommend an upgrade to NINA-B1 series (open CPU) or NINA-B2 series (u-connectXpress).
ODIN-W2	All	
NINA-W15	All	
NINA-B2	All	
NINA-W10	All	
NINA-B50	All	
LILY-W1	All	
EMMY-W1	All	
JODY-W1	All	Mitigation in place with a minimum key length of 7 octets
JODY-W2	All	
JODY-W3	All	
JODY-W4	All	
JODY-W5	All	
MAYA-W1	All	
MAYA-W2	All	
MAYA-W3	All	

2 Type

- ☐ Product status change
- ☐ Hardware/component change
- ☐ Firmware/software update
- ☐ Label change
- ☐ Documentation update
- ☐ Certification information
- ☒ Security advisory
- ☐ Other

3 Description

The Bluetooth SIG (BT-SIG) has published a security notice [1] regarding a novel vulnerability named BLUFFS (Bluetooth Forward and Future Secrecy Attacks and Defenses).

This vulnerability affects all products with support for Bluetooth "Classic" (BR/EDR). All products based on the newer Bluetooth LE (Low Energy) are not affected, neither in isolation nor in products supporting both variants.

The vulnerability requires that an attacker is within wireless range of two vulnerable Bluetooth devices. The vulnerability also requires that a session key first must be broken, typically with brute-force techniques, before past, current and future sessions can be attacked, employing the novel techniques discovered as part of BLUFFS.

Despite this vulnerability affecting all products with support for Bluetooth Classic, the primary mitigation to fix the vulnerability, known as KNOB [3], is available already since 2019.

At the time of the publication of this advisory, we have no evidence that this vulnerability or its variants have been exploited in any of our products.

4 Vulnerability details

As quoted from the white paper of the researcher who discovered the vulnerability, BLUFFS is a set of MITM (Man-in-the-middle) "*attacks breaking Bluetooth's forward and future secrecy by targeting session establishment*" [2]. What this implies in layman's terms is that a session key must first be broken, typically with brute-force techniques, before past, current and future sessions can be attacked. Attackers need to be "*within wireless range of two vulnerable Bluetooth devices initiating an encryption procedure using a link key obtained using BR/EDR Secure Connections pairing procedures*" (1).

Past (recorded) sessions which used that same key can then be decrypted and current/future sessions using the same key can also be decrypted and even tampered with live, e.g. by injecting malicious traffic or spoofing the identity of a previously authenticated endpoint. The set of attacks relies on the ability of the attacker to brute-force a key and to force the reuse of that same key. The attack method allowing an attacker to force the reuse of past keys is part of the discoveries in BLUFFS, whereas brute-forcing is not a new discovery nor a new method in itself. An attacker can, in still vulnerable implementations, rely on previously discovered vulnerabilities to force keys of shorter lengths which are easier to brute-force.

5 Customer impact and recommended action

The primary mitigation in u-blox's current products is already in place due to fixes to a previous vulnerability known as KNOB [3]. This is in line with the recommendation from the Bluetooth SIG, which notes that "*the impact may be limited by [...] ensuring sufficient key entropy to make session key reuse of limited utility to an attacker*" [1]. In practice, the minimum encryption key length is hard coded to 7 octets following the previous and current recommendations – except for a single older product which uses a minimum of 5 octets as noted in Affected products. An upgrade for that product can be considered.

6 General security recommendations

As a general security measure, u-blox strongly recommends protecting network access to devices with appropriate mechanisms. For Bluetooth specifically, the information and guidance provided in u-blox's Application note on Bluetooth Security [4] is recommended.

7 Future work

The researcher gives additional advice with regards to the security protocols described within the Bluetooth standard, with architectural as well as specific technical improvements that may be incorporated in the standard or implementations thereof to alleviate the full vulnerability, including the issues around future and forwards secrecy. Currently u-blox is not aware of any implementation that is considering the inclusion of these additional measures. It is speculated that the measures will not be commonplace until they are adopted by the Bluetooth Special Interest Group (SIG) and included in a later revision of the standard.

8 Classification method

The vulnerability classification has been performed by using the CVSS Common Vulnerability Scoring System (CVSS) in version 3.1 (CVSS v3.1). See also https://www.first.org/cvss/. The CVSS is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

9 Additional information

For Espressif-based products (NINA-B2, NINA-W10, NINA-W15) additional information can be found in their advisory [5].

A full analysis from the researcher can be found in the published whitepaper [2].

u-blox investigated the vulnerability under ID CORSEC-5094.

10 Related documentation

[1] Bluetooth SIG, Security Notice

[2] Antonioli, D. (2023). "BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses" DOI: 10.1145/3576915.3623066

[3] u-blox, "Bluetooth security, Application Note", UBX-16022676, Appendix A.1 "KNOB", CVE-2019-9506

[4] u-blox, "Bluetooth security, Application Note", UBX-16022676

[5] Espressif, "Security Advisory Concerning the Bluetooth BLUFFS Vulnerability", AR2023-010