Security Advisory

Title	Security Advisory Concerning the Bluetooth BLUFFS Vulnerability
Issue Date	2024/01/18
Advisory Number	AR2023-010
Serial Number	CVE-2023-24023
Version	V1.0

Issue Summary

The Bluetooth Special Interest Group (Bluetooth SIG) has issued a security notice regarding the "Bluetooth Forward and Future Secrecy Attacks and Defenses (BLUFFS)" vulnerability disclosed by **Daniele Antonioli**. BLUFFS is tracked with CVE-2023-24023.

The BLUFFS attacks affect both Bluetooth Classic security modes: Legacy Secure Connections (LSC) and Secure Connections (SC). For Bluetooth devices that are already paired using LSC, the vulnerability allows Man in The Middle (MITM) attacks across encrypted sessions. For Bluetooth devices supporting SC, the attacks enable Bluetooth impersonation (BIAS) to downgrade SC to LSC, bypassing the authentication procedure through role switching.

Additionally, BLUFFS uses the Key Negotiation of Bluetooth (KNOB) vulnerability to weaken encryption keys, making it easier for hackers to use brute force attacks to decrypt them. During the brute force attack, the attacker can store session data which can be decrypted once the key is cracked. BLUFFS also exploits flaws in the LSC key derivation algorithm, forcing subsequent sessions to use the previously compromised key. This makes it easy to decrypt the session data.

Bluetooth SIG notes in its security notice that the BLUFFS vulnerability exists in versions of the Bluetooth Core Specification from version 4.2 to version 5.4. The notice proposes mitigations to reduce the impact of this vulnerability but does not present a definitive solution.

Impact Analysis

As BLUFFS attacks target Bluetooth Classic devices, only the ESP32 series of products at Espressif are affected. As the attacks affect Bluetooth at the architectural level, they are effective regardless of the ESP-IDF releases. Until Bluetooth SIG provides a fundamental solution to the issue, refusing SC degradation in sessions and ensuring sufficient key entropy can effectively mitigate the impact of BLUFFS attacks.

Regarding the BLUFFS vulnerability, the following countermeasures have been implemented for ESP32:

1. **KNOB vulnerability fix:** A patch addressing the KNOB vulnerability has been applied. The patch requires the encryption key length for LSC sessions to be at least 7 octets, which makes it challenging for attackers to crack the encryption key in real-time. This fix is available in the currently maintained ESP-IDF release branches (from v4.3 to v5.2, master).

2. **BIAS vulnerability fix:** For information related to the BIAS vulnerability, please refer to Espressif's security advisory AR2021-004. The BIAS vulnerability patch has been introduced to the ESP-IDF Bluedroid protocol stack to prevent the peer device from downgrading a secure connection. It is important to note that for Bluetooth secure connections, ESP32 does not provide any configuration options or interfaces. Furthermore, this patch requires the peer device to undergo at least one authentication, which makes it difficult for attackers to bypass the authentication procedure.

ESP-IDF BIAS Affected Versions:

ESP-IDF Branch	Affected Commit IDs	Affected ESP-IDF Versions
master	All commits before 042fd5f8	N/A
release/v5.0	All commits before 650b6653	v5.0
release/v4.4	All commits before 07518cf4	v4.4 ~ v4.4.3
release/v4.3	All commits before 60e28180	v4.3 ~ v4.3.4

ESP-IDF BIAS Patched Versions:

ESP-IDF Branch	Fixed Commit ID	Fixed IDF Version
master	042fd5f8	N/A

release/v5.1	042fd5f8	v5.1
release/v5.0	650b6653	v5.0.1
release/v4.4	07518cf4	v4.4.4
release/v4.3[1]	60e28180	v4.3.5

[1] ESP-IDF v4.3 has reached end-of-life. New features, bug fixes, and security fixes will no longer be supported on this branch.

Subsequent planned measures include:

API for configuring minimum key length: Espressif plans to provide an API that allows users to configure the minimum key length for device security. For users with higher security requirements, this API will enable the configuration of stronger encryption session keys, thereby increasing the time and computing power required for a brute-force attack.

Recommendations for Application Developers

When you develop the ESP32 series of products or upgrade ESP-IDF versions used on ESP32, it is recommended to use patched ESP-IDF versions mentioned above or versions after the patch commit. If you encounter problems during the upgrade process, please provide the IDF version or Commit ID to Espressif. We will confirm and handle related matters as soon as possible.