Silicon Labs Security Advisory

A-00000388

Subject: Security Advisory for Bluetooth Pairing Method Confusion

CVSS Severity: High

Base Score: 8.0, High
Temporal Score: 7.8, High
Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C&version=3.1

Impacted Products:

- Bluetooth LE-capable products including
  - EFR32-based SoCs and associated modules.
  - BT121 and BT122 modules.
  - RS9113 and RS9116 SoCs and associated modules.

Technical Summary

- This is a vulnerability in the Bluetooth protocol.
- A man-in-the-middle attack is possible on devices supporting the LE legacy pairing method.
- An attacker can downgrade the pairing method used by the one of the peers from LE secure connections to LE legacy pairing and determine the passkey entered by that user.
- The following CVE has been reserved for this vulnerability CVE-2022-25836.

Fix/Work Around:

- Product implementations can avoid this vulnerability by requiring LE secure connections to peer devices.
- In cases where enforcing LE secure connections is not feasible, warn the user that they may be entering a passkey for a less secure connection and may be vulnerable to a man-in-the-middle attack.

Guidelines on our security vulnerability policy can be found at https://www.silabs.com/security
For Silicon Labs Technical Support visit: https://www.silabs.com/support

Notice: The contents of this Notification are provided exclusively for the internal use of the recipient in support of devices supplied by Silicon Labs and shall not be shared with or distributed to any third parties. This Notification shall not be posted on any blog, website, board or social media. The contents are for general information only and do not purport to be comprehensive. While Silicon Labs provides this information in good faith and makes every effort to supply correct, current and high-quality guidance, Silicon Labs provides all materials (including this document) solely on an "as is" basis without warranty of any kind. Silicon Labs disclaims all express and implied warranties. In no event shall Silicon Labs be liable for any damages whatsoever, including direct, indirect, incidental, consequential, lost profits or special damages related to or arising from the adequacy, accuracy, completeness or timeliness of this document or its contents, even if Silicon Labs has been advised of the possibility of such damages. Nothing in this Notice excludes any liability for death or personal injury caused by negligence, or for fraud or intentional misrepresentation. By accepting or using the information contained in this Notification, the recipient agrees to that this Notification and its use are governed by the laws of the State of Texas, excluding its conflicts of law's provisions.