

Silicon Labs Security Advisory

A-00000445

Subject: Security Advisory for Bluetooth LE Denial of Service when receiving invalid sequence of packets

CVSS Severity: Medium

Base Score: 6.5, Medium

Temporal Score: 5.9, Medium

Vector String: [CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C](#)

Impacted Products:

- EFR32MG and EFR32BG based modules and associated SoCs running Bluetooth SDK versions as follows:
 - 3.3.2 or earlier, delivered as part of Gecko SDK version 4.0.2 or earlier.
 - 3.2.3 or earlier, delivered as part of Gecko SDK version 3.2.3 or earlier.
 - 3.1.2 or earlier, delivered as part of Gecko SDK version 3.1.2 or earlier.
 - 3.0.2 or earlier, delivered as part of Gecko SDK version 3.0.2 or earlier.
 - 2.13.10 or earlier, delivered as part of Gecko SDK version 2.7.11 or earlier.

Technical Summary

- A crash and reset may occur in any of the impacted products mentioned above when a peer device continues sending data after receiving a terminate indication packet.
- The following CVE has been reserved for this vulnerability, [CVE-2022-24941](#).

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.

Fix/Work Around:

- An improvement has been made to the SDK to discard any packets received while a connection is being closed.
- Users should upgrade to the fixed version of the SDK based on the current version of the SDK being used as summarized in the table below:

Gecko SDK branch	Fixed Version
3.3.x	4.1.0 (or higher)
3.2.x	3.2.4 (or higher)
3.1.x	3.1.3 (or higher)
3.0.x	3.0.3 (or higher)
2.7.x	2.7.12 (or higher)

- Gecko SDK 3.x users can upgrade as follows:
 - Through Simplicity Studio, select “Install,” then under the “SDK” tab, select Gecko SDK - 32-bit and Wireless MCUs version 4.1.0 or higher
 - Select the installed version of Gecko SDK in “Launcher” under “General Information / Preferred SDK”
 - Rebuild your projects or reflash demo software using the new SDK
- Gecko SDK 2.x users can upgrade as follows:
 - In Simplicity Studio, go to the help menu and select the ‘update software’ menu item. Click the ‘manage installed packages’ button, select the SDKs tab, find the ‘Bluetooth SDK’ section, and click the ‘Update’ button.

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.



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>

Attribution:

Silicon Labs would like to thank Dewitt Seward for bringing this internal discovery via fuzz testing to our attention.

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.