

Silicon Labs Security Advisory

A-00000449

Subject: Potential heap overflow for certain configurations of Mbed TLS 2.18.1 and later

CVSS Severity: High

Base Score: 8.6, High

Temporal Score: 8.2, High

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

Impacted Products:

- Gecko MCUs such as EFX32 SoCs and associated modules using Gecko SDK 3.1 AND LATER that meet all three of the following criteria may be impacted:
 - The device is configured to operate as a DTLS server
 - The device has the MBEDTLS_SSL_DTLS_CONNECTION_ID option enabled AND
 - The device has $MBEDTLS_SSL_CID_IN_LEN_MAX > 2 * MBEDTLS_SSL_CID_OUT_MAX$

Technical Summary:

- The SSL Client ID feature allows clients to quickly reference previous connections in order to save overhead in re-establishing a connection and is typically used by “sleeping” IoT end devices that may disconnect during periods of inactivity.
- Due to a defect in Mbed TLS versions 2.18.1 and later, incoming client ID requests can overflow into heap space if $MBEDTLS_SSL_CID_IN_LEN_MAX$ is larger than $2 * MBEDTLS_SSL_CID_OUT_MAX$
- Note that the SSL Client ID feature is an optional optimization that is not required in order to operate as a DTLS server and that this optional feature is disabled by default in Gecko SDK

Fix/Work Around:

- As of this notification, there is no officially published fix from Mbed TLS. Until an official patch from Mbed TLS is released, it is recommended to leave `MBEDTLS_SSL_DLS_CONNECTION_ID` disabled
- If SSL Client IDs are required for your solution, ensure that $MBEDTLS_SSL_CID_IN_LEN_MAX$ does not exceed $2 * MBEDTLS_SSL_CID_OUT_MAX$

Attribution:

- This vulnerability was reported directly by Mbed TLS to the Trusted Stakeholder Notification distribution list

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>

1 [silabs.com](https://www.silabs.com) | A-00000449 – Potential heap overflow for certain configurations of Mbed TLS 2.18.1 and later

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.