Silicon Labs Security Advisory

A-00000450

Subject: Side channel leakage in Mbed TLS RSA operations allows private key recovery

CVSS Severity: Medium

Base Score: 5.3, Medium
Temporal Score: 4.7, Medium
Vector String: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:W/RC:R

Impacted Products:

- EFx32 SoCs and modules that meet all of the following criteria may be impacted:
    - Running Mbed TLS version 2.x before 2.28.2 or 3.x before 3.3.0 (to be delivered in a later GSDK)
    - Running a user application that performs RSA private key calculations using protected private keys

Technical Summary:

- This vulnerability is tracked in CVE-2022-46392, summarized below.
    - An issue was discovered in Mbed TLS before 2.28.2 and 3.x before 3.3.0. An adversary with access to precise enough information about memory accesses (typically, an untrusted operating system attacking a secure enclave) can recover an RSA private key after observing the victim performing a single private-key operation, if the window size (MBEDTLS_MPI_WINDOW_SIZE) used for the exponentiation is 3 or smaller.
- This vulnerability allows a malicious thread running on a device to recover an RSA private key by observing memory accesses. This is only a valuable attack if the RSA private key is protected from that thread using key wrapping or OS level memory partitioning.
- Series 0 and Series 1 devices do not support key wrapping and Series 2 devices do not natively support RSA for key wrapping.
- The default MBEDTLS_MPI_WINDOW_SIZE in the Gecko SDK is 6, so GSDK projects that do not lower the window size to 3 or lower are not affected by this vulnerability.
- RSA usage in Mbed TLS for each of the stacks included with Gecko SDK are described in the table below:

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.

Stack	Impact
AWS IoT	Uses Mbed TLS for RSA with default window size 6, not impacted
Bluetooth	Does not use RSA
OpenThread	Does not use RSA
Wi-SUN	Does not use RSA
Z-Wave and Z-Wave Long Range	Does not use RSA
Z/IP Gateway	Uses Openssl for RSA, not impacted
Zigbee EmberZNet	Does not use RSA

Fix/Workaround:

- Impacted devices may increase the MBEDTLS_MPI_WINDOW_SIZE to 4 or higher to mitigate this vulnerability. Doing so will improve performance but increase the memory footprint.
- Impacted devices may update Mbed TLS from 2.x to 2.28.2 or higher or from 3.x to 3.3.0 or higher to fix the issue. Mbed TLS v3.3.0 or higher is scheduled to be delivered with a future GSDK release.

Certification Impact:

- Certified products that mitigate the issue in software will need to be recertified.

Discovery Source:

- This vulnerability was brought to our attention by TrustedFirmware.org

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.