Silicon Labs Security Advisory

A-00000442

Subject: Security Advisory for TrustZone Debug Access Permission bits cause TPIU access failure

CVSS Severity: Medium

Base Score: 4.6, Medium
Temporal Score: 4.4, Medium
Vector String: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C

Impacted Products:

- Gecko MCUs such as EFx32 SOCs and associated modules using SE Firmware 1.2.13, 2.2.0 or earlier whose TrustZone Invasive Debug Lock (DBGLOCK) AND Non-Invasive Debug Lock (NIDLOCK) Bits are set

Technical Summary:

- Due to an undocumented behavior in ARM Cortex-M33, setting the TrustZone Debug Access Permission (DAP) DBGLOCK AND NIDLOCK bits unexpectedly causes the M33 to stall when accessing the Trace Port Interface Unit (TPIU) due to a lack of clock input to the TPIU. As a result, the M33 becomes nonresponsive waiting on a ready signal from the peripheral.
- Customers that DO NOT manipulate the TPIU from within application code are **unaffected** by this defect.
- This is a defect in host processor clock integration and the SE or VSE are **unaffected** while the host processor is stalled waiting for access on the TPIU.
- TrustZone DAP bits can be set by either SE Mailbox or DCI interface, regardless of debug state and do not require authentication via Secure Debug challenge response. Once set, they cannot be unset again until the device is erased.
- Note that TrustZone DAP bits operate in addition to, and are not required by, Silicon Labs Secure Debug, and that setting DBGLOCK and NIDLOCK can be achieved regardless of Secure Debug Unlock state. However, be aware that certain configurations of SE Firmware prior to 1.2.14 and 2.2.1 allow a user to place their device into the affected configuration such that future TPIU access will cause the M33 to become nonresponsive.
- A potential malicious user with physical access may be able to latch a device in the nonresponsive state by setting DBGLOCK and NIDLOCK over an available debug interface. However, exploiting this behavior is impractical: attackers with physical access can simply destroy the chip itself to the same effect

Fix/Work Around:

- To avoid being affected by this defect, users should upgrade SE Firmware to versions 1.2.14 or later, or 2.2.1 or later, as soon as these firmware versions become available. **Note that as of this publication these versions may not yet be available,** but should be released in an upcoming GSDK release. For more details please contact support.
- Note that TrustZone Support is in Beta for all Silicon Labs products at this time, and customers should avoid setting TrustZone DAP bits, especially DBGLOCK and NIDLOCK, prior to the 1.2.14 and 2.2.1 releases.
- If your solution requires TrustZone DAP Locks to be enabled, please contact Silicon Labs support for further guidance by filing a ticket via the support portal link
- Applications with TrustZone DAP Locks set can avoid this defect by avoiding TPIU access in application code. For example, the SWO Debug plugin in GSDK will cause this fault if the TrustZone DBGLOCK and NIDLOCK are set. To disable SWO Debug follow the steps below:
    1. Access your device's .slcp file
    2. Under "Software Components" access Platform>Driver>SWO Debug and click "Uninstall"
    3. Clean and Rebuild your project
- A device with Permanent Lock enabled (Device Erase is disabled), in the non-responsive state caused by this defect is NOT RECOVERABLE. If you plan on using TrustZone DAP, ensure your application does not access the TPIU:
    1. Familiarize yourself with ARM's TPIU Programmer's Model, then search and disable any references to the TPIU—most typically the SWO—as described, above
- In the event Permanent Debug Lock is NOT enabled (Device Erase is enabled) and you believe setting TrustZone DAP bits, or TPIU access has caused your device to become nonresponsive, your device can be recovered by issuing a device erase command:

```
commander security erasedevice
```

Attribution:

- Discovered by Silicon Labs internal testing

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