Silicon Labs Security Advisory

A-00000441

Subject: A production misconfiguration in EFM32PG22 allows software to unlock the debug port without erasing flash or RAM in devices with date codes earlier than 2239

CVSS Severity: Medium

Base Score: 7.2, High
Temporal Score: 6.3, Medium
Vector String: CVSS:3.1/AV:P/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:T/RC:C

Impacted Products:

- EFM32PG22 SoCs with date code earlier than 2239 and running SE firmware v1.2.12 or earlier may be impacted

Technical Summary:

- A bug in the EFM32PG22 production flow resulted in devices being manufactured with an invalid security configuration. This invalid configuration allows user code running on the Cortex-M33 to potentially gain root privileges.
- Exploiting this vulnerability requires confidential proprietary knowledge of the EFM32PG22's design and implementation.
- An attacker with code execution privileges on the device could potentially gain root privileges on the device, unlock the debug port, or access protected memory.

Fix/Work Around:

- The production test program was fixed September 23, 2022. Devices manufactured with date code greater than or equal to 2239 are not vulnerable.
- A patch will be available in VSE firmware v1.2.13, scheduled to be released December 7, 2022. Potentially vulnerable devices should upgrade to VSE firmware v1.2.13 before deployment. Deployed devices with a field upgrade option can use VSE firmware v1.2.13 to patch the vulnerability.

Attribution:

- This vulnerability was discovered by internal Silicon Labs 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