

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.

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.



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>

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.