



201027915 EFR32MG22, BG22, FG22 Virtual Secure Element Firmware Update

Bulletin Issue Date: 10/27/2020

Effective Date: 10/27/2020

Description of Change

Silicon Labs announces Virtual Secure Element (VSE) firmware version 1.2.6 for EFR32MG22, EFR32BG22, EFR32BG22C112 and EFR32FG22 SoCs.

Reason for Change

This is a firmware update to address a vulnerability. Details are covered in Security Advisory - A-00000114 and also in Software Advisory - A-00000117.

VSE firmware version 1.2.5 and earlier have the following issues:

1. A device whose VSE firmware has been successfully upgraded at least once can become inoperable if the upgrade file is removed from flash after the upgrade and the device is subjected to a large cumulative number of resets. The exact number of reset cycles before failure varies due to process variations and operating temperature but would typically range between 50,000 and 200,000 cycles. It is imperative that this fix be applied to every device to avoid latent failures.
2. In the event of a momentary power failure whose duration is sufficient to cause only a few specific RAM bits to lose state, the POR boot process can terminate in a hard fault.

VSE v1.2.6 fixes both issues. Silicon Labs manufacturing production has been updated as of October 19 , 2020, to apply VSE version 1.2.6 so that new production devices will not have this issue.

Product Identification

Existing Part #
EFR32BG22C222F352GM32-C
EFR32BG22C222F352GM40-C
EFR32BG22C222F352GN32-C
EFR32BG22C224F512GM32-C
EFR32BG22C224F512GM40-C
EFR32BG22C224F512GN32-C
EFR32BG22C224F512IM32-C
EFR32BG22C224F512IM40-C
EFR32BG22C112F352GM32-C
EFR32MG22C224F512GN32-C
EFR32MG22C224F512IM32-C
EFR32MG22C224F512IM40-C
EFR32FG22C121F512GM32-C
EFR32FG22C121F512GM40-C
EFR32BG22C222F352GM32-CR
EFR32BG22C222F352GM40-CR
EFR32BG22C222F352GN32-CR
EFR32BG22C224F512GM32-CR
EFR32BG22C224F512GM40-CR
EFR32BG22C224F512GN32-CR
EFR32BG22C224F512IM32-CR
EFR32BG22C224F512IM40-CR
EFR32BG22C112F352GM32-CR
EFR32MG22C224F512GN32-CR
EFR32MG22C224F512IM32-CR
EFR32MG22C224F512IM40-CR
EFR32FG22C121F512GM32-CR
EFR32FG22C121F512GM40-CR
EFR32FG22C121F256GM32-C

EFR32FG22C121F256GM40-C
EFR32FG22C121F256GM32-CR
EFR32FG22C121F256GM40-CR

This change is considered a minor change which does not affect form, fit, function, quality, or reliability. The information is being provided as a customer courtesy.

Please contact your local Silicon Labs sales representative with any questions about this notification. A list of Silicon Labs sales representatives may be found at <http://www.silabs.com>.

Customer Actions Needed:

Devices with VSE firmware version 1.2.5 or earlier, should be updated to firmware version 1.2.6 or later. For more information on identifying the EFR32xG22 security firmware version, see AN1222. Firmware updates can be done during the product manufacturing process or via an over the air update for products in the field. For more information on upgrading the SE firmware, see UG266.

User Registration

Register today to create your account on Silabs.com. Your personalized profile allows you to receive technical document updates, new product announcements, "how-to" and design documents, product change notices (PCN) and other valuable content available only to registered users. <http://www.silabs.com/profile>



Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOModem®, Micrium, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.



Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701

<http://www.silabs.com>