



# 200225730 xGM210L and xGM210P Secure Element Firmware Version 1.2.1

**Bulletin Issue Date:** 2/25/2020

**Effective Date:** 2/25/2020

## Description of Change

Silicon Labs announces Secure Element (SE) firmware version 1.2.1 for MGM210 and BGM210 modules.

## Reason for Change

A vulnerability has been discovered which allows code running on the Cortex-M33 to erase or program flash that is reserved for SE use. Although security measures such as Secure Boot and variable encoding make it difficult to implement a productive exploit of this flaw, it is possible that such an exploit could be used to gain access to sensitive data or to bypass security features.

This vulnerability has been addressed in SE firmware version 1.2.1. Modules with trace code of 2007 (YYWW) and later are updated with SE firmware version 1.2.1 and will not have this vulnerability.

Devices with SE firmware version 1.2.0 or earlier, should be updated to firmware version 1.2.1 or later. For more information on identifying the EFR32xG21 and xGM210 security firmware version, see AN1222 or refer to the emlib SE\_getStatus() command - <https://docs.silabs.com/mcu/latest/mgm21/group-SE>. 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.

## Product Identification

Existing Part #  
BGM210L022JIF1  
BGM210L022JIF1R  
BGM210L022JIF2  
BGM210L022JIF2R  
BGM210L022JNF1  
BGM210L022JNF1R  
BGM210L022JNF2  
BGM210L022JNF2R  
BGM210LA22JIF1  
BGM210LA22JIF1R  
BGM210LA22JIF2  
BGM210LA22JIF2R  
BGM210LA22JNF1  
BGM210LA22JNF1R  
BGM210LA22JNF2  
BGM210LA22JNF2R  
BGM210P022JIA1  
BGM210P022JIA1R  
BGM210P022JIA2  
BGM210P022JIA2R  
BGM210P022JNA2  
BGM210P022JNA2R  
BGM210P032JIA1  
BGM210P032JIA1R  
BGM210P032JIA2  
BGM210P032JIA2R  
BGM210P032JNA2  
BGM210P032JNA2R  
BGM210PA22JIA1  
BGM210PA22JIA1R

BGM210PA22JIA2  
BGM210PA22JIA2R  
BGM210PA22JNA2  
BGM210PA22JNA2R  
BGM210PA32JIA1  
BGM210PA32JIA1R  
BGM210PA32JIA2  
BGM210PA32JIA2R  
BGM210PA32JNA2  
BGM210PA32JNA2R  
MGM210L022JIF1  
MGM210L022JIF1R  
MGM210L022JIF2  
MGM210L022JIF2R  
MGM210L022JNF1  
MGM210L022JNF1R  
MGM210L022JNF2  
MGM210L022JNF2R  
MGM210LA22JIF1  
MGM210LA22JIF1R  
MGM210LA22JIF2  
MGM210LA22JIF2R  
MGM210LA22JNF1  
MGM210LA22JNF1R  
MGM210LA22JNF2  
MGM210LA22JNF2R  
MGM210P022JIA1  
MGM210P022JIA1R  
MGM210P022JIA2  
MGM210P022JIA2R  
MGM210P022JNA2  
MGM210P022JNA2R  
MGM210P032JIA1  
MGM210P032JIA1R  
MGM210P032JIA2  
MGM210P032JIA2R  
MGM210P032JNA2  
MGM210P032JNA2R  
MGM210PA22JIA1  
MGM210PA22JIA1R  
MGM210PA22JIA2  
MGM210PA22JIA2R  
MGM210PA22JNA2  
MGM210PA22JNA2R  
MGM210PA32JIA1  
MGM210PA32JIA1R  
MGM210PA32JIA2  
MGM210PA32JIA2R  
MGM210PA32JNA2  
MGM210PA32JNA2R

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:

Review Secure Element (SE) firmware version 1.2.1

### 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>