Application Report

Boot Image Manager (BIM) Potential Security Vulnerabilities in CC13x2, CC26x2, CC2640R2 Devices

TI-PSIRT-2020-080064

Publication date: May 24, 2021

Summary

The following outlines potential security vulnerabilities of Boot Image Manager (BIM) software for CC13x2, CC26x2 and CC2640R2 devices that support secure firmware updates (on-chip and off-chip) and secure boot operations:

1. [On-chip only] BIM only authenticates the user application image, not the persistent application image. BIM could incorrectly run a malicious user application image if the image is located at the flash page > 0 and the image type information has been compromised by setting the Over The Air (OAD) image type to OAD_IMG_TYPE_PERSISTENT_APP.
   a. CVSS base score: 7.9
   b. CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:T/RC:C
   c. Remediation: Authenticate the persistent application image before booting into it and use pre-defined location of the persistent application image.
2. *2A*: [Off-chip only] BIM allows the user application image to be located in any of the flash pages; however, an implementation bug causes image authenticity check to always point to image residing at the address zero. An attacker could potentially append malicious code to a valid image at address 0x0 with a valid signature and bypass check of malicious code that is appended at a different flash page with this potential vulnerability.

   2B: [Off-chip and on-chip] Once BIM validates the user application image, it jumps to the program entry address of the user application image based on the image header data. However, BIM does not validate the program entry address whether or not it is within the authenticated user application image region. BIM could potentially execute an unauthenticated firmware image, as it supports user application images to be located at any flash page.

   [Off-chip only] Vulnerabilities 2A and 2B can be combined to potentially execute unauthenticated malicious code appended to a valid image in a different flash page.

   a. CVSS base score: 7.3
   b. CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:T/RC:C
   c. Remediation: [Off-chip] Ensure the image authentication region is identical to the actual image location. [Off-chip and on-chip] Add a check to confirm the program entry address is within the authenticated image region.

Affected products and versions

The BIM software in the below SDKs are affected:

- SIMPLELINK-CC13X2-26X2-SDK (v4.30.00.54 and prior versions)
- SIMPLELINK-CC2640R2-SDK (v4.30.00.08 and prior versions)
  – Note: #2A is not applicable to CC2640R2

Potentially impacted features

The potential vulnerabilities can impact CC13x2, CC26x2 and CC2640R2 devices running affected TI BIM versions for supporting on-chip and off-chip OAD in the applications.

- CC13x2/CC26x2 OAD user's guide
- CC2640R2 OAD user's guide

Suggested mitigations

The following SDK releases address the potential vulnerabilities:

Affected SDK	SDK version with mitigations	SDK release dates with mitigations
SIMPLELINK-CC13X2-26X2-SDK	V4.40.xx.xx (4Q20 official SDK)	January 2021
SIMPLELINK-CC2640R2-SDK	v5.10.xx.xx (1Q21 official SDK)	April 2021

Revision history

- Version 1.0 Initial publication

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265