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
   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.

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
   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:

<table>
<thead>
<tr>
<th>Affected SDK</th>
<th>SDK version with mitigations</th>
<th>SDK release dates with mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMPLELINK-CC13X2-26X2-SDK</td>
<td>V4.40.xx.xx (4Q20 official SDK)</td>
<td>January 2021</td>
</tr>
<tr>
<td>SIMPLELINK-CC2640R2-SDK</td>
<td>v5.10.xx.xx (1Q21 official SDK)</td>
<td>April 2021</td>
</tr>
</tbody>
</table>

Revision history

- Version 1.0 Initial publication