Application Report

Potential Heap Overflow Vulnerabilities in TI Z-Stack Zigbee Cluster Library (ZCL) Parsing Functions

TI-PSIRT-2020-070058

Publication date: January 22, 2021

Summary

The following outlines potential security vulnerabilities in the TI Z-Stack Zigbee Cluster Library (ZCL) software for CC26x2/13x2, CC2630/50 and CC2530/1/8 devices:

ZCL Foundation (on network):

CVSS base score: 6.0

CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:H/E:F/RL:O/RC:C

The potential ZCL Foundation vulnerabilities can be compromised with the following preconditions:

1. The target device must be commissioned and authenticated onto a Zigbee network. The target could be any node in the network, including a network leader device (e.g. Trust Center, if in a centralized security network).
2. The attacking device must also be commissioned and authenticated onto the same network.

In Zigbee network systems with the above conditions, the attacking device can send malformed ZCL Foundation frames over-the-air to cause the memory overflow on the target device, which may lead to undefined behavior (e.g. device hard fault) or potential remote code execution. The following ZCL Foundation APIs (found in zcl.c) are vulnerable:

zclParseInReadRspCmd()	ZCL Read Attributes Response Command
zclParseInWriteCmd()	ZCL Write Attributes Command
zclParseInConfigReportCmd()	ZCL Configure Reporting Command
zclParseInReadReportCfgRspCmd()	ZCL Read Reporting Configuration Response Command
zclParseInReportCmd()	ZCL Report Attributes Command

The mitigation for the potential issues with these commands is to sanitize the input data length in the payload.

ZCL Touchlink Commissioning (off network):

CVSS base score: 7.8

CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

The potential ZCL Touchlink Commissioning vulnerabilities can be compromised with the following preconditions:

1. The attacking device must be placed in very close physical proximity to the target device in order for Touchlink Commissioning (proximity-based commissioning) to work.
2. The attacking device must be placed into Touchlink target mode, with a malicious payload enabled. The attacking device will now wait for a Touchlink initiator to send a scan request.
3. A user with authenticated access to the target device must interact with it and manually initiate network commissioning with Touchlink initiator mode enabled.

If a vulnerable device is acting as a Touchlink initiator, a ZCL Touchlink Device Information Response Command sent from a Touchlink Target (attacker) to the Touchlink initiator (target) may contain a malformed payload that can potentially cause memory overflow on the target device, which may lead to undefined behavior (e.g. device hard fault) or potential remote code execution.

The mitigation for the potential issue with this command is to sanitize the input data length in the payload.

ZCL Touchlink Commissioning (on network):

CVSS base score: 6.0

CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:H/E:F/RL:O/RC:C

The following ZCL Touchlink Commissioning vulnerabilities can be compromised with the following preconditions:

1. The target device is commissioned and authenticated onto a distributed security Zigbee network formed by Touchlink Commissioning. The target could be any node in the network.
2. The attacking device must also be commissioned and authenticated onto the same network.

In Zigbee network systems with the above conditions, the attacking device can send malformed ZCL Touchlink Commissioning frame over-the-air to cause memory overflow on the target, which may lead to undefined behavior (e.g. device hard fault) or potential remote code execution. The following ZCL Touchlink APIs (found in bdb_tl_commissioning.c) are vulnerable:

bdbTL_ProcessInCmd_GetGrpIDsRsp()	Get Group Identifiers Response Command
bdbTL_ProcessInCmd_GetEPListRsp()	Get Endpoint List Response Command
bdbTL_ProcessInCmd_DeviceInfoRsp()	Device Information Response Command

The mitigation for the potential issues with these commands is to sanitize the input data length in the payload.

Affected products and versions

- Z-Stack component of SimpleLink™ CC13x2_26x2 SDK (all versions)
- SimpleLink Zigbee SDK Plugin (deprecated)
- Z-Stack Home 1.2.2a for CC2630/CC2650/CC2530/1/8 (deprecated)
- Z-Stack 3.0.x for CC2530/1/8 (deprecated)

Potentially impacted features

Zigbee Cluster Library software

Suggested mitigations

The following SDK releases address the potential vulnerability:

Affected SDK	SDK version with mitigations	SDK releases with mitigations
SIMPLELINK-CC13X2-26X2-SDK	SIMPLELINK-CC13X2-26X2-SDK_4.40.00.44	Jan 2021

External references

- Ruben Santamarta, Principal Security Consultant at IOActive

Revision history

- Version 1.0 Initial publication

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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, 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 (https:www.ti.com/legal/termsofsale.html) 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.

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