Application Report

SimpleLink™ CC13XX, CC26XX, CC32XX and MSP432E4 Integer Overflow Issues

TI-PSIRT-2020-100074

Publication date: April 29, 2021

Summary

Below are the integer overflow issues in the SimpleLink™ CC13XX, CC26XX, CC32XX and MSP432E4 SDKs that could potentially lead to issues like heap overflows and remote code execution. These potential vulnerabilities cannot typically be used to compromise the device without another vulnerability allowing control of the function call parameters.

CVEID	Description	CVSS score (v3.0)	CVSS vector
CVE-2021-22636	Potential integer overflow in TI-RTOS 'malloc'	7.4	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2021-27429	Potential integer overflow in TI-RTOS 'HeapTrack_alloc'	7.4	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2021-27502	Potential integer overflow in TI-RTOS 'HeapMem_allocUnprotected'	7.4	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2021-27504	Potential integer overflow in FreeRTOS POSIX 'malloc'	7.4	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Affected products

- CC13XX
- CC26XX
- CC32XX
- MSP432E4XX

Potentially impacted features

- TI-RTOS kernel heap manager
- FreeRTOS POSIX heap manager

Suggested mitigations

The following mitigations are released in the SDKs listed below. It is recommended that customers of affected products apply these suggested mitigations and consider further system-level security measures as appropriate.

- In tirtos/packages/ti/sysbios/rts/MemAlloc.xdt, ti_sysbios_rts_MemAlloc_alloc(), a check was added to return NULL if size + sizeof(Header) overflowed.
- In kernel/tirtos/packages/ti/sysbios/heaps/HeapTrack.c, HeapTrack_alloc(), a check was added to return NULL if size + res + sizeof(HeapTrack_Tracker) overflowed.
- In source/ti/posix/freertos/memory.c, malloc(), a check was added to return NULL if size + sizeof(Header) overflowed.
- In tirtos/packages/ti/sysbios/heaps/HeapMem.c HeapMem_allocUnprotected(), a check was added to return NULL if adjSize overflowed. HeapMem_allocUnprotected() and HeapMem_alloc() were removed from ROM on CC13XX and CC26XX devices.

The following SDK releases address the potential vulnerability:

Affected SDK	SDK version with mitigations	SDK releases with mitigations
CC32XX SDK	CC32XX SDK V4.40.00.07	Jan 2021
SIMPLELINK-CC13X2-26X2-SDK	SIMPLELINK-CC13X2-26X2-SDK V4.40.00	Jan 2021
SIMPLELINK-CC2640R2-SDK	SIMPLELINK-CC2640R2-SDK V4.40.00	Feb 2021
SIMPLELINK-CC13X0-SDK	SIMPLELINK-CC13X0-SDK V4.10.03	Feb 2021

The SimpleLink MSP432E4 SDK does not have a planned SDK update to address the mitigations discussed above due to the legacy nature of its software. The TI-RTOS and FreeRTOS files above are common between the mentioned SDKs. It is recommended that customers patch in the mentioned files from one of the updated SDKs above to the SimpleLink MSP432E4 SDK.

Note: Customers are solely responsible for the security of their products and are encouraged to assess the possible risk of any potential security vulnerability.

Acknowledgment

We would like to thank Omri Ben Bassat and David Atch of Microsoft for working with CISA to report these vulnerabilities to the TI Product Security Incident Response Team (PSIRT).

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