Application Report

SimpleLink™ Wi-Fi® CC32xx/CC31xx SDK and SimpleLink MSP432E4 SDK Integer and Buffer Overflow Issues

TI-PSIRT-2020-100073

Publication date: April 29, 2021

Summary

Below are integer and buffer overflow issues in the SimpleLink™ Wi-Fi® CC32xx SDK and SimpleLink MSP432E4 SDK that could potentially lead to issues like denial of service or 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 (v3.1)	CVSS vector	CC3x2x CC3x3x	CC3100 CC3200	MSP432E4
CVE-2021-22677	Potential integer overflow in 'sl_WlanConnect', 'sl_WlanProfileAdd', and 'sl_WlanProfileUpdate' when trying to connect to a Wi-Fi network with a long name (SSID)	8.4	AV:L/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:H	+	+	
CVE-2021-22673	Potential buffer overflow in 'CdnClient_ConnectFileServer' and 'CdnClient_ReqFileContent'	7.2	AV:N/AC:L/PR:H/ UI:N/S:U/C:H/I:H/A:H	+		
CVE-2021-22675	Potential integer overflow in 'GetEntireFile' when parsing malformed over-the-air (OTA) firmware update file	7.2	AV:N/AC:L/PR:H/ UI:N/S:U/C:H/I:H/A:H	+		
CVE-2021-22679	Potential integer overflow in 'resHeaderNameToHash' on malformed http response	9.8	AV:N/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:H	+		+

Affected products and versions

- SimpleLink Wi-Fi CC32xx SDK 4.30.00.06 and older versions
- SimpleLink MSP432E4 SDK 4.20.00.12 and older versions
- SimpleLink Wi-Fi Plug-in 4.20.00.10 and older versions
- CC3200 SDK v1.5.0 and older versions
- CC3100 SDK v1.3.0 and older versions

Potentially impacted features

- SimpleLink Wi-Fi driver
- OTA
- HTTP client

Suggested mitigations

The updates below have been released in the SimpleLink Wi-Fi CC32xx SDK version 4.40.00.07. It is recommended that customers of affected products apply these suggested mitigations and consider further system-level security measures as appropriate.

1. In wlan.c, sl_WlanConnect, sl_WlanProfileAdd and sl_WlanProfileUpdate, a condition was added that verifies “NameLen > 0”.

2. In OtaHttpClient.c and HttpClient_ParseUrl, a condition was added that verifies the length of the domain name is no longer than the size of ServerNameBuf.
3. In OtaArchive.c and GetEntireFile, a condition was added that verifies FileSize is not bigger than max uint32_t value (0xFFFFFFFF).
4. In HttpClient.c, the logic of resHeaderNameToHash was replaced.

For SimpleLink MSP432E4 SDK mitigation efforts, it is recommended for customers to replace the HttpClient.c within the MSP432E4 SDK with the new version mentioned above in the SimpleLink Wi-Fi CC32xx SDK mitigation (item 4).

For SimpleLink Wi-Fi Plug-in mitigation efforts, it is recommended for customers to replace the wlan.c and httpclient.c within the Wi-Fi Plug-in with the new versions mentioned above from the SimpleLink Wi-Fi CC32xx SDK mitigation (item 1 and item 4). To support the new httpclient.c file, customers must also replace the httpclient.h file within the Wi-Fi Plug-in with the version from the v4.40 CC32xx SDK. Customers should also replace the definition of HttpClient_ParseUrl() function in ota_httpclient.c of the plug-in with the new definition from the OtaHttpClient.c of the SimpleLink Wi-Fi CC32xx SDK mitigation (item 2). Additionally, customers should add the following code between lines 139 and 140 of ota_archive.c in the current Wi-Fi plug-in:

```
If (FileSize >= (uint32_t)MaxUint32_t)
{
 return ARCHIVE_STATUS_ERROR_BUNDLE_CMD_FILE_NAME_MAX_LEN;
}
```

For mitigation in the CC3100 and CC3200 SDKs, it is recommended that customers replace line 88 and line 382 in the wlan.c from the latest SDKs (`VERIFY_PROTOCOL(NameLen <= MAX_SSID_LEN);`) with:

```
VERIFY_PROTOCOL(NameLen >= 0 && NameLen <= MAX_SSID_LEN);
```

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 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