PSIRT Notification

Buffer Overflow in WL18xx MCP Driver

Summary

The TI WiLink WL18xx MCP driver does not limit the number of information elements (IEs) of type XCC_EXT_1_IE_ID or XCC_EXT_2_IE_ID that can be parsed in a management frame. Using a specially crafted frame, a buffer overflow can be triggered that can potentially lead to remote code execution.

Vulnerability

TI PSIRT ID

TI-PSIRT-2022-120160

CVE ID:

CVE-2023-29468

CVSS Score

The CVSS base score for this issue can range from 8.8 to 9.6. The higher base score reflects a Confidentiality and Integrity impact of *High*. However, some systems can have a Confidentiality or Integrity Impact of *Low* depending on the characteristics of the host processor executing the WL18xx MCP driver and whether the disclosure or modification of the memory that can be accessed represents a direct or serious loss.

CVSS vector

- High Score (9.6): CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- Low Score (8.8): CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H

Affected Products

- WILINK8-WIFI-MCP8 version 8.5_SP3 and earlier

Potentially Impacted Features

An attacker within wireless range of a potentially vulnerable device can gain the ability to overwrite memory of the host processor executing the MCP driver.

Suggested Mitigations

In MCP8.5_SP3\WiLink\UWD\src\Services\mlmeParser.c, include the following code starting at line 720:

```
if( rsnIeIdx >= 3 )
{
TRACE(pHandle->hReport, REPORT_SEVERITY_ERROR, "MLME_PARSER: Number of RSN IEs exeeds 3\n");
return TI_NOK;
}
```


Acknowledgments

We want to thank Omri Ben Bassat of Microsoft for reporting this vulnerability to the TI Product Security Incident Response Team (PSIRT).

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