Application Note

Integrated HTTP Server Ping Utility Vulnerability

TI-PSIRT-2021-100117

Publication date: Feb 15, 2022

CVEID: CVE-2021-21966

Summary

The SimpleLink™ CC32xx/CC31xx includes an integrated HTTP server that provides services which can be activated without involving the application processor (services are offloaded from the application processor). Among the HTTP services is a ping utility that can be used to test and troubleshoot network connectivity issues.

When the utility is activated, the device sends a ping with an optional payload buffer. The buffer used to send the payload is not initialized properly and may include sensitive information.

The vulnerability was originally reported on TI's CC3200, but TI has analyzed the potential effect on all SimpleLink Wi-Fi CC32xx/CC31xx generations, and those affected versions are listed below.

Common Vulnerability Scoring System (CVSS) base score: 5.3

CVSS vector:

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Affected products and versions

- CC3100
- CC3200
- CC3120
- CC3220R/CC3220S/CC3220SF
- CC3130
- CC3230S/CC3230SF
- CC3135
- CC3235S/CC3235SF

Potentially impacted features

The vulnerability requires that the integrated HTTP server is enabled and the attacker is connected to the same LAN as the device in order to access the integrated HTTP server services. The attacker must also know the device IP address.

Suggested mitigations

The updates below have been released and fix this vulnerability:

- SimpleLink_cc32xx_sdk_5_30_00_08
  - Products supported: CC3220R/S/SF, CC3120, CC3230S/SF, CC3130, CC3235S/SF, CC3135
  - Service pack versions
    - CC3x20: sp_3.21.0.1_2.7.0.0_2.2.0.7
    - CC3x3x: sp_4.12.0.1_3.7.0.1_3.1.0.26
- CC3100_CC3200_ServicePack_1.0.1.15-2.15.0.1
  - Products supported: CC3100, CC3200
  - Service pack version:
    - servicepack_1.0.1.15-2.15.0.1

Copyright © 2022 Texas Instruments Incorporated

It is recommended that customers of affected products apply these suggested mitigations.

Customers should also consider disabling the integrated HTTP server when not used in order to reduce the attack surface on their products.

Acknowledgment

We would like to thank Cisco Talos team for reporting this vulnerability to the TI Product Security Incident Response Team (PSIRT).

External reference

Talos Vulnerability Report TALOS-2021-1393

Revision history

- Version 1.0 Initial publication

Copyright © 2022 Texas Instruments Incorporated

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
Copyright © 2022, Texas Instruments Incorporated