PSIRT Notification

Enabling Tools Client Mode Leads to Possibility of Bypassing Debug Authentication On CC27xx Devices

Summary

The CC27xx Debug Authentication can be bypassed if both the configurations below are simultaneously enabled:

1. Debug Authentication Mode is enabled in CCFG
2. Tools Client Mode is enabled in *both* CCFG *and* SCFG

Note 1: If Tools Client Mode is enabled in only one of the two configuration modes (CCFG or SCFG), then this vulnerability does not occur. The recommended mitigation below reflects this fact.

Note 2: This vulnerability is not applicable and does not impact customer systems if customers have followed the guidance outlined in the *CC27xx Technical Reference Manual* Section 10.1 *Securely Configuring Your Device* which includes instructions in Section 10.1.4 to disable Tools Client Mode. This guidance also appears in Section 9.1.5 *Flashless Test Mode and Tools Client Mode* which addresses measures to establish the most secure configuration.

Vulnerability

CVE ID

None

CVSS Score

7.6

CVSS Vector

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Affected Products

Device Part Number	Affected Version
CC2745R10-Q1, CC2745R7-Q1, CC2744R7-Q1, CC2745P10-Q1, CC2755R10, CC2755P10	Rev F and former

Potentially Impacted Features

The Debug Authentication can be bypassed via a physical debug interface if both the configurations below are simultaneously enabled:

1. Debug Authentication Mode is enabled in CCFG
2. Tools Client Mode is enabled in *both* CCFG *and* SCFG

Bypassing the debug authentication can affect the security of the application code and data stored in the device's memory. Note that this vulnerability cannot be exploited with remote or local wireless access. Refer to CVSS vector above for further details.

As noted above, this vulnerability is not applicable and does not impact customer systems if customers have followed the guidance outlined in Section 10.1 and Section 9.1.5 of the *CC27xx Technical Reference Manual*.

Suggested Mitigations

Section 10.1 *Guidelines for Securely Configuring Your Device* of the CC27xx Technical Reference Manual instructs customers to *Disable xcfg.permissions.allowToolsClientMode* (Section 10.1.4 *Configure Device Permissions*) prior to deployment to the field.

Tools Client Mode configuration is enabled by default in software examples provided by TI for development purposes. If Debug Authentication is enabled, the issue described above can be avoided by disabling the Tools Client Mode configuration. Following the recommendations in Section 10.1.4 on how to configure device permissions to disable tools Client Mode prior to deployment to the field, and in Section 9.1.5 of the CC27xx Technical Reference Manual on how to establish the most secure configuration, prevents this vulnerability from occurring. The Tools Client Mode feature can be enabled during application development, as required, but is recommended to disable the feature for production devices before deployment to the field.

Tools Client Mode is disabled by writing CCFG_PERMISSION_FORBID in the ccfg.permissions.allowToolsClientMode field of the CCFG.

- For SysConfig-enabled projects, the option *SysConfig* > *Device Configuration* > *Secure Configuration Permissions* > *Allow Tools Client Mode* must be deactivated.
- For Zephyr projects, this configuration is enabled through KConfig symbols set in the prj.conf file. The symbol CC27XX_ALLOW_TOOLS_CLIENT_MODE must be set to *n*.

Disabling only the Tools Client Mode in CCFG is sufficient because the most restrictive configuration between CCFG and SCFG — in this case the *disabled* configuration for CCFG — is applied.

References

- Texas Instruments, *CC27xx SimpleLink™ Wireless MCU* technical reference manual
  - Section 10.1 *Securely Configuring Your Device* includes instructions in Section 10.1.4 to disable Tools Client Mode. This guidance also appears in Section 9.1.5 *Flashless Test Mode and Tools Client Mode*, which addresses measures to take to establish the most secure configuration.

Trademarks

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, 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 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, TI’s General Quality Guidelines, 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. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025