*PSIRT Notification*

# *C2000 DCSM ROM Gadget/ROP Vulnerability*


## Summary

The secure ROM implementation in several C2000 C28-based products can be exploited by an attacker to bypass memory zone protections enforced by the Dual Code Security Mode (DCSM). Attacks on secure memory regions are possible, bypassing the innermost boundary of protections of the DCSM.


## Vulnerability

### TI PSIRT ID

TI-PSIRT-2023-080189

### Definitions

- **Gadget:** A sequence of instructions existing in memory maliciously used by an attacker in a way unintended by the original program. Gadgets are often chained together to work as a simple unit to perform arbitrary computations or functions that serve the attacker's purposes.
- **ROP:** Return-oriented-programming; a method of attack that chains gadgets together by modifying the return address location of the stack memory.
- **PSIRT:** TI's Product Security Incident Response Team oversees the process of accepting and responding to reports of potential security vulnerabilities involving TI semiconductor products, including hardware, software and documentation. For more information, see TI PSIRT.
- **CVSS:** Common Vulnerability Scoring System, maintained by FIRST.

### CVE ID

Not applicable.

### CVSS Base Score

6.7

### CVSS Vector

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

### Affected Products

- TMS320F28003x
- TMS320F2838x
- TMS320F280013x
- TMS320F280015x
- TMS320F28P65x

### Potentially Impacted Features

The following attributes may be affected by this vulnerability:

- Confidentiality and integrity of EXEONLY code in memory.
- Confidentiality and integrity of non-EXEONLY data/code in memory.

### Suggested Mitigations

Enable two features existing on the device:

- **JTAGLOCK**. The JTAG interface should be locked. See the SPRACS4 application report for how to lock the JTAG interface.
- **Zero-pin boot to flash boot method**. The boot method should be programmed to always boot directly to an internal flash boot mode, either “Flash” or “Secure Flash”. See the device’s Technical Reference Manual for details on how to enable.

These two features provide protection from an attacker connecting a debugger or using a bootloader to load code into internal memory. This injected code is required to launch an ROP/gadget attack on secure memory regions. Best cybersecurity coding and testing practices should also be employed on user application code to prevent attackers from loading their code into internal memory. This includes, but is not limited to, secondary bootloaders, firmware update code, and communication stacks.

### Acknowledgments

We would like to thank Zhao Hai from Cyberpeace Tech Co., Ltd. for reporting this vulnerability to the TI Product Security Incident Response Team (PSIRT).

## Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

| DATE | REVISION | NOTES |
|---|---|---|
| November 2023 | * | Initial Release |

# 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