PSIRT Notification

MSP430FR5xxx and MSP430FR6xxx IP Encapsulation Write Vulnerability

Summary

The IP Encapsulation feature of the Memory Protection Unit may not properly prevent writes to an IPE protected region under certain conditions. This vulnerability assumes an attacker has control of the device outside of the IPE protected region (access to non-protect memory, RAM, and CPU registers).

Vulnerability

TI PSIRT ID

TI-PSIRT-2023-040180

CVE ID

Not applicable.

CVSS Base Score

7.1

CVSS Vector

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

Affected Products

- MSP430FR58xx family devices
- MSP430FR59xx family devices
- MSP430FR6xxx family devices

Potentially Impacted Features

This vulnerability allows an attacker to write arbitrary code to an IPE protected region, potentially gaining access to protected code. Applying recommended mitigations may limit the functionality of the code within the IPE protected memory region.

Suggested Mitigations

The attacker needs access to the non-protected regions of the device to exploit this vulnerability. Preventing this access would be the first step in preventing the vulnerability. A combination of the following mitigations can be utilized to prevent the vulnerability.

- Locking of JTAG and BSL interfaces to prevent device access.
- Use the Memory Protection Unit (MPU) to place write protections on the IPE protected region, while locking MPU settings to prevent attackers from removing protections.

Additional security practices are discussed in the MSP Code Protection Features application note.

Acknowledgments

We would like to thank Marton Bognar, Cas Magnus, Jo Van Bulck, and Frank Piessens from KU Leuven University in Belgium for reporting this vulnerability to the TI Product Security Incident Response Team (PSIRT).

External References

Texas Instruments, *MSP Code Protection Features*, application note.

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