Application Note

Physical Security Attacks Against Silicon Devices

TI-PSIRT-2021-100116

Publication date: January 31, 2022

CVEID: None

Summary

Texas Instruments has observed the increasing reports of physical security attacks against silicon devices, and recognizes this problem as an industry-wide issue. These types of attacks require physical access or close proximity to a potentially vulnerable device. Silicon devices (whether made by TI or another silicon vendor) designed without comprehensive mitigations against physical attacks, are potentially vulnerable. Fortunately, since an attacker must obtain physical access to the device, and may even need to make printed circuit board (PCB) modifications, these types of attacks do not, on their own, have the same potential for broad impact and scale as remote attacks. However, a physical attack may lead to information disclosures which may assist in the development of different remote attacks.

Physical attacks include, but are not limited to:

- Fault injection attacks, including voltage spike glitches, electromagnetic pulses, clock glitching injection, overclocking, and focused ion beam attacks
- Side-channel attacks against silicon, including power analysis and electromagnetic analysis

Common Vulnerability Scoring System (CVSS) base score: Can range from 4.8 to potentially as high as 6.1

The higher base score reflects a Confidentiality Impact of “High.” However, some systems may have a Confidentiality Impact of “Low” if the disclosure of the information programmed in the part does not represent a direct or serious loss. Additionally, the higher base score reflects an Attack Complexity of “Low.” However, some physical attacks (e.g., focused ion beam attacks) would be considered to have an Attack Complexity of “High.” In addition, physical controls preventing physical access to the part may raise the Attack Complexity metric for the overall system to “High.” Thus, several factors will impact the CVSS base score of a particular physical attack.

CVSS vector

- **High Score (6.1):** CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
- **Low Score (4.8):** CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N

Affected products and versions

- If a TI product does not have documented mitigations against a specific physical attack, it may be vulnerable.
- If a TI product does have documented mitigations against a specific physical attack and a related vulnerability for that product is confirmed by TI, TI will publish a specific disclosure for that part.

Potentially impacted features

The following are generally known goals of physical attacks against silicon devices:

- Debug unlock,
- cryptographic key extraction, and
- general memory read-out.

Achievement of these goals may result in information disclosure of data stored on the device and may also result in the ability to program or reprogram the device.

Suggested mitigations

General techniques for mitigating physical attacks include the following:

- Physically secure the PCB in an enclosure using locks, security screws, potting, or other similar protections.
- Using sensors to detect the opening of the PCB's enclosure and deleting secrets when an unauthorized access is detected.
- Limiting impact of attack by using unique keys for each device and avoiding storing sensitive information in the device.

Texas Instruments is working to address the security needs of our customers as those needs evolve due to new attack methods. This pursuit includes investigating the addition of physical attack mitigations. If your company has questions about the availability of mitigations in TI parts, please reach out to your TI sales team.

Acknowledgment

We would like to thank researchers from COSIC, KU Leuven for reporting a specific instance of this potential vulnerability to the TI Product Security Incident Response Team (PSIRT).

Revision history

- Version 1.0 Initial publication

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