Security Advisory

Title	Security Advisory Concerning Bypassing Secure Boot and Flash Encryption Using EMFI
Issue Date	2023/07/11
Advisory Number	AR2023-005
Serial Number	CVE-2023-35818
Version	V1.0

Issue Summary

Security researchers from the company **Raelize** and **Technology Innovation Institute (TII)** reported a new vulnerability using EMFI (Electro Magnetic Fault Injection) attack on ESP32 Chip Revision v3.0. Using the EMFI technique, the execution flow in ESP32 can be changed in a controlled way to jump directly into UART Download mode implemented in ROM code. This is possible with Secure Boot (V2) and Flash Encryption features enabled in their Release mode configuration and UART Download mode permanently disabled.

- ### What Is EMFI?

  EMFI is a class of Side Channel Attack which can alter the embedded device behavior by electromagnetic pulses. Using this technique, a sufficiently strong electromagnetic field is applied on the chip surface with the help of an active probe, which may cause fault on the memory surface and thus changing the value held by memory. In some cases, the chip metal shield is also removed to improve the probe performance on the chip surface.

  The challenging part is, to achieve the desired goal, the attacker must find the spatial location on the chip surface by running the experiment for hundreds of thousands of times. If applying this technique may alter the memory content as desired, it could lead to the control of device execution flow.

- **Issue Details**

  An attacker with physical access to the ESP32 device and sophisticated lab equipment would be able to figure out the spatial location on the chip and other EMFI attack parameters like glitch delay and power. This will give an attack vector which could be exploited to influence the CPU PC (Program Counter) value at run time in a controlled way.

  Once PC control capability is achieved using EMFI, it could be used to make PC jump into the part of ROM code which could be exploited, e.g., UART Download mode, and thus bypassing security features.

  For manipulating the PC in a controlled way, the address must be programmed in the ESP32 flash storage. In the presence of security features like Secure Boot and Flash Encryption, researchers carefully used the debug information from ROM serial logs, and iteratively found the way to inject the arbitrary address into CPU PC to reproduce the attack.

- **Impact Analysis**

  EMFI attack on ESP32 provides the attacker with a capability to influence the PC value at the CPU context level, irrespective of the Secure Boot and Flash Encryption status. Also, in ESP32 ROM implemented UART Download mode entry point is not hardened to resist against the fault injection attack.

  Using these two vulnerabilities, an attacker could bypass the security features, make the CPU enter ROM UART Download mode, and would be able to communicate over the UART communication channel. This allows one to load and execute arbitrary stub code (internal memory only) or read decrypted contents from flash memory.

  This is a semi-invasive attack, which requires a higher skill set and precision to find and target specific spatial and temporal locations on the chip. The success rate is low, which is a deterrent for attackers.

Mitigation

There is no immediate mitigation available for this issue. Here are a few general recommendations to follow:

These attacks need substantial effort, advanced skills, expensive and sophisticated lab equipment to be carried out successfully on a device. If each device is provisioned with a unique secret key tied to that specific device identity, then the attacker cannot scale it to an entire class of devices, making this attack less attractive.

Several Espressif products are available in System-in-Package (SiP) form-factor with flash pins terminated internally. SiP such as ESP32-PICO-V3 and ESP32-PICO-V3-02 can help to make this attack difficult to execute as the attack requires frequent manipulation of the flash contents using an external flash programmer.

Other Espressif Products

This attack is applicable to ESP32 Chip Revision v3.0 and v3.1. Please note that the prior ESP32 Chip Revisions cannot permanently disable UART Download mode and hence they were already vulnerable to this attack (reason to not consider them here).

ESP32-S2, ESP32-C3, ESP32-S3 and all our future chips have countermeasures available in ROM code to prevent fault injection attacks, including the one discussed in this advisory.

Credits

We would like to thank **Cristofaro Mune** and **Niek Timmers** from **Raelize** and **Jeroen Delvaux** and **Mario Romero** from **Technology Innovation Institute (TII)**, for reporting this vulnerability and assisting us with the disclosure.