# CVE Detail – CVE-2019-15894

An issue was discovered in Espressif ESP-IDF 2.x, 3.0.x through 3.0.9, 3.1.x through 3.1.6, 3.2.x through 3.2.3, and 3.3.x through 3.3.1. An attacker who uses fault injection to physically disrupt the ESP32 CPU can bypass the Secure Boot digest verification at startup, and boot unverified code from flash. The fault injection attack does not disable the Flash Encryption feature, so if the ESP32 is configured with the recommended combination of Secure Boot and Flash Encryption, then the impact is minimized. If the ESP32 is configured without Flash Encryption then successful fault injection allows arbitrary code execution. To protect devices with Flash Encryption and Secure Boot enabled against this attack, a firmware change must be made to permanently enable Flash Encryption in the field if it is not already permanently enabled.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.12779

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-755: Improper Handling of Exceptional Conditions

## Affected Products

* cpe:2.3:a:espressif:esp-idf:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:espressif:esp-idf:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:espressif:esp-idf:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:espressif:esp-idf:\*:\*:\*:\*:\*:\*:\*:\*