Information note

Topic **Security Advisory for Espressif AES Key Extraction Using Voltage Glitch**
UBXDOC-465451970-4905 C1-Public

Author Martin Furmanski

Date 12 June 2026

1 Affected products

The method has been confirmed on ESP32-S3 chips by Espressif but is believed to also affect ESP32 and ESP-C6 chips due to the nature of the exploit. See the linked advisory[1] from Espressif for further details.

Product name/series	Variants	Remarks
NORA-W1	All	open CPU with ESP32-S3 Confirmed by Espressif on chip.
NORA-W2	All	ExpressLink with ESP32-S3 Confirmed by Espressif on chip. N.B: product is NRND
NINA-W1	All	u-connectXpress with ESP32 Not confirmed, but likely.
NINA-B2	All	u-connectXpress with ESP32 Not confirmed, but likely.
NINA-W4	All	open CPU with ESP32-C6 Not confirmed, but likely.

2 Type

- ☐ Product status change
- ☐ Hardware/component change
- ☐ Firmware/software update
- ☐ Label change
- ☐ Documentation update
- ☐ Certification information
- ☒ Security advisory
- ☐ Other

3 Summary

Researchers have discovered a new vulnerability affecting the AES hardware block. The vulnerability relies on a fault injection (voltage glitch) and several additional steps after which the AES key used within the AES hardware block can be extracted. There is at this time no CVE assigned and Espressif has given the advisory[1] an ID of AR2026-005. For most (or even all) customers the risk should be low enough to not warrant any further action.

4 Vulnerability details

The vulnerability requires lots of time and expertise, as well as prolonged physical access to the device. See the linked advisory from Espressif for further details.

5 Customer impact and recommended action

Espressif points to the impact especially on long-lived (AES) session keys, as used for example during secure communications with long sessions. Similarly, a flash encryption key is generally also a long-lived key. The user has some control over the length of communications sessions and putting an upper limit on the session length could in theory lessen the impact. Additional (and unproven) attack steps, building upon the confirmed attack path, would be required for such an exploit chain. In u-connectXpress modules, with additional steps, this could help towards an attack on the flash. Assets typically stored on the flash (encrypted) are user secrets or derived keys.

Cautious customers are advised to analyze their products and deployments to understand whether the vulnerability poses a security risk sufficient to warrant further action. The complexity of any (unconfirmed) full attack chain and the requirements on time, tools and skills should for most customers put this vulnerability below the bar where action is warranted (i.e. under a risk-based process - like the Cyber Resilience Act). If you have stronger requirements, please get in touch with u-blox through the regular support channel to explore further options.

Espressif similarly makes an assessment of low impact on deployed systems.

6 Related documentation

[1] https://documentation.espressif.com/AR2026-005_Security_Advisory_Concerning_AES_Key_Recovery_Using_Voltage_Fault_Injection_on%20ESP32-S3_EN.pdf