CVE Request 1985899 for CVE ID Request

From CVE Request <CVE-Request@mitre.org>

To fr0mthecloud@proton.me

Date Friday, January 30th, 2026 at 2:23 PM

Thank you for the following submission. It will be reviewed by a CVE Assignment Team member.

Vulnerability Type: Other or Unknown

Suggested description of the vulnerability:
A hardware-level security violation exists in the Texas Instruments SN27xxx Series Battery Fuel Gauge IC (integrated into the Apple iPhone 14 & 15 Pro Max). The One-Time Programmable (OTP) security fuses designed to permanently disable manufacturing/debug interfaces remain unprogrammed (unblown) in production hardware. This "Unrestricted Factory Mode" state permits persistent JTAG/debug access, unauthorized I2C/SMBus bus master elevation, and the execution of undocumented factory test commands via the Secure Processing Unit (SPU). The exploit allows for the mounting of a reserved memory partition, masked via manipulation of the battery capacity reporting, and operates on the Always-On (AON) power domain, persisting across OS updates and factory resets.

Changes, additions, or updates to your request can be sent to the CVE Team by replying directly to this email. Please do not change the subject line, which allows us to effectively track your request.

CVE Assignment Team

M/S M300, 202 Burlington Road, Bedford, MA 01730 USA

[A PGP key is available for encrypted communications at

http://cve.mitre.org/cve/request_id.html]

{CMI: MCID15612789}