Re: [scr1985899] Texas Instruments SN27xxx Series Battery Fuel Gauge IC - All Versions

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

To fr0mthecloud@proton.me

CC CVE Request<cve-request@mitre.org>

Date Sunday, February 1st, 2026 at 12:04 AM

> [Suggested description]
> The Texas Instruments SN27xxx series Battery Fuel Gauge IC has a
> hardware-level security violation (this IC is, for example, integrated
> into the Apple iPhone 14 and 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,
> I2C/SMBus bus master elevation, and the execution of undocumented
> factory test commands via the Secure Processing Unit (SPU).
> Exploitation allows the mounting of a reserved memory partition, masked
> through manipulation of battery capacity reporting, and would operate on
> the Always-On (AON) power domain, persisting across OS updates and
> factory resets.
>
> ----------
>
> [VulnerabilityType Other]
> Unfused OTP security registers (hardware debug access)
>
> ----------
>
> [Vendor of Product]
> Texas Instruments
>
> ----------
>
> [Affected Product Code Base]
> Texas Instruments SN27xxx Series Battery Fuel Gauge IC - All Versions
> Apple iPhone 14 Pro Max - All Versions
> Apple iPhone 15 Pro Max - All Versions
>
> ----------
>
> [Reference]

> https://kb.cert.org/vince/comm/case/3086/
>
> ----------
>
> [Has vendor confirmed or acknowledged the vulnerability?]
> true
>
> ----------
>
> [Discoverer]
> Joseph Raymond Goydish II
>
> ----------
>
> [Reference]
> https://ti.com

Use CVE-2026-25251.

--
CVE Assignment Team
M/S M300, 202 Burlington Road, Bedford, MA 01730 USA
[A PGP key is available for encrypted communications at
https://cve.mitre.org/cve/request_id.html]