Apple Extends CoreGraphics Fix for Exploited CVE-2026-86950 to Older iPhones and iPads



Apple has backported a fix for CVE-2026-86950, a high-severity CoreGraphics flaw exploited in real attacks, to older devices. Patches for newer devices were released last month.

- The flaw is tracked as CVE-2026-86950 and carries a CVSS score of 8.8.
- It is an out-of-bounds write in CoreGraphics that can lead to arbitrary code execution.
- Exploitation requires processing a maliciously crafted file.
- Apple confirms the flaw was exploited in real-world attacks.
- Fixes now cover older iPhones and iPads; the original patches came last month.

Apple has released fixes for an actively exploited vulnerability to older iPhones and iPads, extending

protection that was first issued for other devices last month.

What happened

The flaw, tracked as **CVE-2026-86950** (CVSS 8.8), is an out-of-bounds write in CoreGraphics. If a device processes a maliciously crafted file, an attacker could achieve arbitrary code execution. The source reports that the vulnerability has been exploited in real-world attacks.

The latest update is a backport: the same fix is now available for older hardware that did not receive it in the original release.

Why it matters

Organisations often keep older iPhones and iPads in service, including shared devices, spare units and devices held by staff on bring-your-own-device schemes. These are the devices most likely to have missed the first round of patches. Because exploitation is confirmed and the trigger is simply opening or processing a file, unpatched devices are a practical exposure.

The source does not give details on the attackers, targets or the specific device models and software versions affected, so teams should consult Apple's own advisory for the exact list.

Recommended approach

Treat this as a prioritised patching task. Confirm which managed and personal devices fall under the older-device update, apply the fix, and verify completion through your device management tooling rather than relying on user action.

What to do now

1. Inventory all iPhones and iPads, including older models, shared units and BYOD devices that access corporate data.
2. Check Apple's official advisory for CVE-2026-86950 to confirm which models and OS versions receive the backported fix.
3. Push the update through MDM and report on compliance; escalate devices that remain unpatched.
4. Restrict or isolate devices that cannot be updated from email and sensitive systems.
5. Remind staff to avoid opening unexpected files and to report suspicious attachments to the security team.