

PSA: Dozens of critical security updates are waiting for your iPhone and Mac

Apple released the first major OS 26 updates earlier this week and they include lots of patches.

By [Michael Simon](#) Executive Editor, Macworld NOV 8, 2025 5:59 am PST



Image: Foundry

On Monday, Apple released the [first updates to its 2026 range of operating systems](#), and they include [numerous new features](#) that iPhone and Mac users will love, including interface tweaks, new gestures, and Spotlight enhancements.

But even more important to the billion-plus devices getting the updates is a full slate of security patches. The first update following a major OS release is always an important one for squashing bugs and ironing out performance issues, but there

are also nearly 100 security updates for macOS Tahoe and another few dozen for the iPhone.

None of the vulnerabilities has been reported to have been exploited in the wild, but several of them pose critical risks to sensitive information. Among the long list fixes, these caught our eye.

App Store

- Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later
- Impact: An app may be able to fingerprint the user
- Description: A permissions issue was addressed with additional restrictions.
- CVE-2025-43444: Zhongcheng Li from IES Red Team of ByteDance

Apple Account

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe

- Impact: A malicious app may be able to take a screenshot of sensitive information in embedded views
- Description: A privacy issue was addressed with improved checks.
- CVE-2025-43455: Ron Masas of BreakPoint.SH, Pinak Oza

Apple TV Remote

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later
- Impact: A malicious app may be able to track users between installs
- Description: The issue was addressed with improved handling of caches.
- CVE-2025-43449: Rosyna Keller of Totally Not Malicious Software

Contacts

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe
- Impact: An app may be able to access sensitive user data
- Description: A logging issue was addressed with improved data redaction.
- CVE-2025-43426: Wojciech Regula of SecuRing (wojciechregula.blog)

Find My

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe
- Impact: An app may be able to fingerprint the user
- Description: A privacy issue was addressed by moving sensitive data.
- CVE-2025-43507: iisBuri

Finder

- Available for: macOS Tahoe
- Impact: An app may bypass Gatekeeper checks
- Description: A logic issue was addressed with improved validation.
- CVE-2025-43348: Ferdous Saljooki (@malwarezoo) of Jamf

Notes

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe
- Impact: An app may be able to access sensitive user data
- Description: A privacy issue was addressed by removing the vulnerable code.
- CVE-2025-43389: Kirin (@Pwnrin)

Photos

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe
- Impact: An app may be able to access user-sensitive data
- Description: A permissions issue was addressed with additional sandbox restrictions.
- CVE-2025-43405: an anonymous researcher

Safari

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe
- Impact: An app may be able to bypass certain Privacy preferences
- Description: A privacy issue was addressed by removing sensitive data.
- CVE-2025-43502: an anonymous researcher

Stolen Device Protection

- Available for: iPhone 11 and later
- Impact: An attacker with physical access to a device may be able to disable Stolen Device Protection
- Description: The issue was addressed by adding additional logic.
- CVE-2025-43422: Will Caine

WebKit

- Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later; macOS Tahoe
- Impact: An app may be able to monitor keystrokes without user permission
- Description: The issue was addressed with improved checks.
- WebKit Bugzilla: 300095

- CVE-2025-43495: Lehan Dilusha Jayasinghe

If you haven't updated your iPhone, iPad, or Mac yet, go do it now. To update your device, head over to Settings on the iPhone or System Settings on the Mac, then *General* and *Software Update*, and follow the prompt.

Author: [Michael Simon](#), Executive Editor, Macworld

Michael Simon has been covering Apple for more than 20 years. He started covering rumors with Spymac when the iPod was the iWalk, and has owned nearly every iPhone Apple has ever made. He lives in Connecticut with his wife, son, and far too many gadgets.