tom's guide

Stop everything and update your iPhones, iPads and Macs — Apple issues critical fix for zero-day exploits

News By Amber Bouman published April 1, 2025

If you've been holding on to your older Apple devices, it's time to go update them now.

On Monday, Apple issued critical fixes for three zero-day exploits that mainly target older iOS and macOS devices. The vulnerabilities have come under active exploitation in the wild on older model devices and previous versions of the operating systems.

In addition to the backported fixes, Apple additionally released iOS 18.4 and iPadOS 18.4 to patch 62 flaws, macOS Sequoia 15.4 to fix 131 flaws, tvOS 18.4 for 36 flaws, visionOS 2.4 for 38 flaws and Safari 18.4, which corrects 14 flaws.

You may like:

- Apple just patched its first zero-day flaw of the year — update your iPhone and Mac right now
- iOS 18.3.1 — update your iPhone right now to fix critical zero-day vulnerability

Though none of these newly disclosed shortcomings have come under active exploitation, users are — as always — recommended to update their devices to the latest version in order to protect their devices against potential threats.

What are the zero-day vulnerabilities?

The three zero-day vulnerabilities are:

CVE-2025-24085, which has a CVSS score of 7.3. It's a use-after-free bug in the Core Media component.

It would permit malicious applications already installed on the device to elevate privileges. It has now been fixed in maxOS Sonoma 14.7.5, macOS Ventura 13.7.5 and iPadOS 17.7.6

…

CVE-2025-24200 with a CVSS score of 4.6. It uses an authorization issue in the Accessibility component to make it possible for a malicious user to disable the USB Restricted Mode on locked devices during a physical cyber attack. It has been fixed in iOS 15.8.4, iPadOS 15.8.4, iOS 16.7.11 and iPadOS 16.7.11

CVE-2025-24201 has a CVSS score of 8.8 and is an out-of-bounds write issue in the WebKit component. It could allow an attacker to craft malicious web content in a way that could break out of the Web Content sandbox. It has been fixed on iOS 15.8.4, iPadOS 15.8.4, iOS 16.7.11 and iPadOS 16.7.11

…