مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

# Security Updates - Apple

Tracking #:432317713

Date:16-09-2025

TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apple has released security updates to address multiple vulnerabilities in its products. The updates address a wide range of vulnerabilities across critical components such as Kernel, WebKit, Bluetooth, CoreMedia, Safari, and Sandbox, some of which could allow sensitive data exposure, sandbox escapes, denial-of-service attacks, or remote code execution via malicious web or media content.

## TECHNICAL DETAILS:

Apple has released security updates addressing multiple vulnerabilities across its ecosystem, including iOS 26 and macOS Tahoe, iOS 18.7macOS Sequoia 15.7,macOS Sonoma 14.8. Given the nature of the flaws—particularly those in WebKit, Kernel, and Bluetooth—there is a heightened risk of remote exploitation and data leakage. Organizations and individuals are strongly advised to update affected devices immediately.

**Details of Key Vulnerabilities:**

- **Kernel (CVE-2025-43359)** – Logic flaw may cause network sockets to bind improperly, potentially exposing services.
- **WebKit (CVE-2025-43272, CVE-2025-43343, CVE-2025-43342, CVE-2025-43368)** – Processing malicious web content can lead to crashes, memory corruption, or unauthorized access to sensor information.
- **Bluetooth (CVE-2025-43354, CVE-2025-43303)** – Logging flaws may allow sensitive data exposure.
- **LaunchServices (CVE-2025-43362)** – Could allow apps to monitor keystrokes without user permission.
- **Sandbox & Shortcuts (CVE-2025-43329, CVE-2025-43358)** – Apps or shortcuts may escape sandbox restrictions.
- **Notes (CVE-2025-43203)** – Physical attackers may bypass protections to view images in locked notes.
- **Text Input (CVE-2025-24133)** – Sensitive keyboard suggestions may appear on the lock screen.
- **Safari (CVE-2025-31254)** – URL validation flaw may enable redirection attacks.
- **SQLite (CVE-2025-6965)** – Memory corruption vulnerability inherited from open-source component.

**Software Updates Details:**

| Name | Available for |
|---|---|
| iOS 26 and iPadOS 26 | 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 |

| | |
|---|---|
| iOS 18.7 and iPadOS 18.7 | 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 |
| iOS 16.7.12 and iPadOS 16.7.12 | iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation |
| iOS 15.8.5 and iPadOS 15.8.5 | iPhone 6s (all models), iPhone 7 (all models), iPhone SE (1st generation), iPad Air 2, iPad mini (4th generation), and iPod touch (7th generation) |
| macOS Tahoe 26 | Mac Studio (2022 and later), iMac (2020 and later), Mac Pro (2019 and later), Mac mini (2020 and later), MacBook Air with Apple silicon (2020 and later), MacBook Pro (16-inch, 2019), MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports), and MacBook Pro with Apple silicon (2020 and later) |
| macOS Sequoia 15.7 | macOS Sequoia |
| macOS Sonoma 14.8 | macOS Sonoma |
| tvOS 26 | Apple TV HD and Apple TV 4K (all models) |
| watchOS 26 | Apple Watch Series 6 and later |
| visionOS 26 | Apple Vision Pro |
| Safari 26 | macOS Sonoma and macOS Sequoia |
| Xcode 26 | macOS Sequoia 15.6 and later |

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends installing the latest versions released by Apple.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://support.apple.com/en-us/100100