مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Apple

Tracking #:432317928

Date:04-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apple has released security updates across its product ecosystem addressing numerous vulnerabilities across core system components including WebKit, Kernel, Apple Neural Engine, and multiple privacy-related frameworks.

TECHNICAL DETAILS:

Apple has released multiple security updates across its ecosystem addressing numerous vulnerabilities across core system components including WebKit, Kernel, Apple Neural Engine, and multiple privacy-related frameworks.

Several vulnerabilities were identified in WebKit, Apple's core browser component, enabling potential remote code execution through malicious web content. Others affected privacy modules, exposing users to risks of data leakage or tracking.

No active in-the-wild exploits have been reported at the time of release, but given the critical nature of WebKit bugs, prompt patching is strongly advised.

Key Vulnerability Highlights

1. CVE-2025-43442 – Accessibility Data Exposure
A permissions issue allowed apps to determine what other applications were installed on a device. Apple restricted permissions to prevent cross-app enumeration.

2. CVE-2025-43455 – Apple Account Privacy Leak
A privacy flaw in embedded views could allow malicious apps to capture screenshots of sensitive information. Improved validation now blocks such behavior.

3. CVE-2025-43447 & CVE-2025-43462 – Apple Neural Engine Memory Corruption
Memory handling issues could cause system instability or kernel corruption. Apple hardened memory management for the Neural Engine framework.

4. CVE-2025-43379 – AppleMobileFileIntegrity Data Access Bypass
A flaw in symbolic link validation could allow apps to access protected user data. Validation processes have been improved.

5. CVE-2025-43407 & CVE-2025-43448 – Sandbox Escape in Assets / CloudKit
Apps could potentially break out of their sandbox environment due to insufficient entitlement validation. Both issues now mitigated through stricter sandbox controls.

6. CVE-2025-43426 – Contacts Data Exposure
Insufficient logging redaction could expose sensitive data. Apple enhanced data sanitization within system logs.

7. CVE-2025-43350 – Lock Screen Content Leak (Control Center)
Attackers could view restricted content from the lock screen. Additional permission restrictions have been applied.

8. CVE-2025-43398 – Kernel Memory Issue
An app could cause system termination due to improper memory handling. Kernel-level improvements were introduced to prevent DoS conditions.

9. CVE-2025-43413 – libxpc Network Visibility Flaw
A sandboxed app could observe network connections system-wide. Apple added further sandbox isolation to mitigate this exposure.

10. CVE-2025-43496 – Mail Drafts Privacy Violation
Remote images could be loaded even when disabled in settings. Updated logic ensures the user's "Load Remote Images" preference is enforced.

11. CVE-2025-43389, CVE-2025-43391, CVE-2025-43500 – Unauthorized Data Access in Notes, Photos, and Sandbox Profiles
Several privacy flaws could expose user data or preferences. Apple removed vulnerable code and enhanced privacy handling.

12. Multiple WebKit Vulnerabilities (CVE-2025-43421 through CVE-2025-43503)
Numerous vulnerabilities in WebKit could lead to process crashes, arbitrary code execution, address bar spoofing, cross-origin data theft, or keystroke monitoring.
Most issues involved use-after-free, buffer overflow, and memory corruption errors. Apple improved input validation, memory safety, and state management across the engine.

13. CVE-2025-43422 – Stolen Device Protection Bypass
Attackers with physical access could disable Apple's Stolen Device Protection. The issue was fixed by adding logic enforcement to block unauthorized changes.

14. CVE-2025-43452 – Text Input Data Exposure on Lock Screen
Keyboard suggestions could display sensitive data while locked. iOS now restricts prediction options in the locked state.

15. CVE-2025-43454 – Siri Lock Failure
An issue could cause devices to remain unlocked persistently. Apple corrected the flaw with improved state handling.

16. CVE-2025-43460 – Status Bar Information Leak
Attackers with physical access could view sensitive data from a locked device. Logic flaws were patched with stricter checks.

17. CVE-2025-43392 – WebKit Canvas Data Exfiltration
Cross-origin image data could be read via crafted web content. Apple implemented cache-handling improvements to prevent image exfiltration.

Software Updates Details:

Name	Available for
iOS 26.1 and iPadOS 26.1	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 26.1	macOS Tahoe
macOS Sequoia 15.7.2	macOS Sequoia
macOS Sonoma 14.8.2	macOS Sonoma
tvOS 26.1	Apple TV HD and Apple TV 4K (all models)
watchOS 26.1	Apple Watch Series 6 and later
visionOS 26.1	Apple Vision Pro
Safari 26.1	macOS Sonoma and macOS Sequoia
Xcode 26.1	macOS Sequoia 15.6 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply updates Immediately across all managed Apple platform.

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-ae/100100