مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Apple

Tracking #:432317953

Date:06-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apple has released iOS 18.7.2 and iPadOS 18.7.2 addressing over 25 security vulnerabilities across multiple system components for older models.

TECHNICAL DETAILS:

Apple has released iOS 18.7.2 and iPadOS 18.7.2 addressing over 25 security vulnerabilities across multiple system components, including WebKit, Kernel, Siri, Notes, and Model I/O. The flaws range from information disclosure and sandbox escapes to memory corruption and denial-of-service vulnerabilities. Some of these issues could be exploited by malicious applications or crafted web content to execute arbitrary code, exfiltrate sensitive information, or track users without consent.
Given the potential for remote exploitation via WebKit (Safari) and app-level privacy bypasses, users and enterprises are strongly urged to update all compatible iPhones and iPads immediately.

Affected Components, CVEs, and Impacts:

Component	CVE ID(s)	Impact
Accessibility	CVE-2025-43442	An app may be able to identify what other apps a user has installed
App Store	CVE-2025-43444	An app may be able to fingerprint the user
Audio	CVE-2025-43423	An attacker with physical access to an unlocked device paired with a Mac may be able to view sensitive user information in system logging
Camera	CVE-2025-43450	An app may be able to learn information about the current camera view before being granted camera access
CloudKit	CVE-2025-43448	An app may be able to break out of its sandbox
CoreText	CVE-2025-43445	Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory
Find My	CVE-2025-43507	An app may be able to fingerprint the user
Installer	CVE-2025-43444	An app may be able to fingerprint the user
Kernel	CVE-2025-43398	An app may be able to cause unexpected system termination
Mail	CVE-2025-43496	Remote content may be loaded even when the “Load Remote Images” setting is turned off
MetricKit	CVE-2025-43365	An unprivileged process may be able to terminate a root process
Model I/O	CVE-2025-43383, CVE-2025-43384, CVE-2025-43385, CVE-2025-43386	Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory
Model I/O	CVE-2025-43377	An app may be able to cause a denial-of-service
Notes	CVE-2025-43389	An app may be able to access sensitive user data
On-device Intelligence	CVE-2025-43439	An app may be able to fingerprint the user
Safari	CVE-2025-43493	Visiting a malicious website may lead to address bar spoofing
Safari	CVE-2025-43503	Visiting a malicious website may lead to user interface spoofing

Shortcuts	CVE-2025-43499	An app may be able to access sensitive user data
Siri	CVE-2025-43454	A device may persistently fail to lock
Siri	CVE-2025-43399	An app may be able to access protected user data
Spotlight	CVE-2025-43418	An attacker with physical access to a locked device may be able to view sensitive user information
WebKit	CVE-2025-43438	Processing maliciously crafted web content may lead to an unexpected Safari crash
WebKit	CVE-2025-43434	Processing maliciously crafted web content may lead to an unexpected Safari crash
WebKit	CVE-2025-43433	Processing maliciously crafted web content may lead to memory corruption
WebKit	CVE-2025-43431	Processing maliciously crafted web content may lead to memory corruption
WebKit	CVE-2025-43441	Processing maliciously crafted web content may lead to an unexpected process crash
WebKit	CVE-2025-43435	Processing maliciously crafted web content may lead to an unexpected process crash
WebKit	CVE-2025-43429	Processing maliciously crafted web content may lead to an unexpected process crash
WebKit	CVE-2025-43443	Processing maliciously crafted web content may lead to an unexpected process crash
WebKit	CVE-2025-43495	An app may be able to monitor keystrokes without user permission
WebKit Canvas	CVE-2025-43392	A website may exfiltrate image data cross-origin

Security Update:

- iOS 18.7.2 and iPadOS 18.7.2-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

RECOMMENDATIONS:

- Users and enterprises are strongly urged to update all compatible iPhones and iPads immediately to the updated version.

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/125633