مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Apple Devices

Tracking #:432319215

Date:30-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Apple has released security updates to remediate numerous security vulnerabilities affecting supported iPhone and iPad devices.

TECHNICAL DETAILS:

Apple has released iOS 26.5.2 and iPadOS 26.5.2 to remediate numerous security vulnerabilities affecting supported iPhone and iPad devices. The update addresses vulnerabilities across critical components including Kernel, WebKit, WebRTC, Web Extensions, IOGPUFamily, libxslt, and WebKit Storage.

Affected Platforms:

- iPhone 11 and later
- iPad Pro 11-inch (1st generation and later)
- iPad Pro 12.9-inch (3rd generation and later)
- iPad Air (3rd generation and later)
- iPad (8th generation and later)
- iPad mini (5th generation and later)

Vulnerability Details:

- CVE-2026-43743 – Race Condition
- CVE-2026-43724 – Kernel Memory Write
- CVE-2026-43722 – Information Disclosure
- CVE-2026-39868 – Kernel Memory Corruption
- CVE-2026-43706 – Double Free
- CVE-2026-43703 – Memory Handling
- CVE-2026-43704 – Use-After-Free
- CVE-2026-43700 – Cross-Origin Information Disclosure
- CVE-2026-43735 – Cross-Origin Data Exfiltration
- CVE-2026-43734 – Use-After-Free
- CVE-2026-43726 – Use-After-Free
- CVE-2026-43699 – Memory Handling
- CVE-2026-43742 – Path Validation
- CVE-2026-43732 – Use-After-Free
- CVE-2026-43731 – Memory Corruption
- CVE-2026-43715 – Use-After-Free
- CVE-2026-43727 – Out-of-Bounds Access
- CVE-2026-43725 – Sandbox Bypass
- CVE-2026-43663 – Memory Handling
- CVE-2026-39872 – Memory Handling
- CVE-2026-43712 – Memory Handling
- CVE-2026-43716 – Out-of-Bounds Access
- CVE-2026-43676 – Information Disclosure
- CVE-2026-43740 – Permission Issue
- CVE-2026-43713 – Cross-Origin Data Exfiltration
- CVE-2026-43708 – Memory Corruption

- CVE-2026-43707 – Type Confusion
- CVE-2026-43705 – Sandbox Bypass
- CVE-2026-43701 – Out-of-Bounds Write
- CVE-2026-43745 – Use-After-Free
- CVE-2026-43720 – Clipboard Hijacking
- CVE-2026-43721 – State Management
- CVE-2026-28979 – Out-of-Bounds Access
- CVE-2026-43718 – Stack Overflow
- CVE-2026-43717 – Use-After-Free
- CVE-2026-43746 – Use-After-Free

Fixed Version:

- iOS 26.5.2 and iPadOS 26.5.2

RECOMMENDATIONS:

Immediate Actions:

- Organizations managing Apple devices should prioritize deployment of these updates to reduce exposure to web-based attacks, privilege escalation attempts, and denial-of-service conditions.

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/127594