مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Apple

Tracking #:432318654

Date:25-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apple released security updates across its entire product ecosystem, addressing multiple vulnerabilities affecting iOS, iPadOS, macOS, tvOS, watchOS, visionOS, and Safari.

TECHNICAL DETAILS:

Apple released security updates across its entire product ecosystem, addressing multiple vulnerabilities affecting iOS, iPadOS, macOS, tvOS, watchOS, visionOS, and Safari. The vulnerabilities range from information disclosure and denial-of-service (DoS) to sandbox escape, kernel memory corruption, and web-based attacks. Several issues could allow attackers to exploit devices via malicious apps, crafted web content, or privileged network positions.

Vulnerability Details

- **CVE-2026-28865 – 802.1X**
  Network traffic interception from privileged network position
- **CVE-2026-28877 – Accounts**
  Unauthorized access to sensitive user data
- **CVE-2026-28895 – App Protection**
  Bypass of biometric protection using passcode (physical access required)
- **CVE-2026-28879 – Audio**
  Use-after-free leading to application crash via malicious web content
- **CVE-2026-28822 – Audio**
  Type confusion causing unexpected app termination
- **CVE-2026-28874 – Baseband**
  Remote attacker-triggered application crash
- **CVE-2026-28875 – Baseband (iPhone 16e)**
  Buffer overflow leading to denial-of-service
- **CVE-2026-28894 – Calling Framework**
  Remote denial-of-service via crafted input
- **CVE-2026-28866 – Clipboard**
  Unauthorized access to sensitive user data
- **CVE-2026-20690 – CoreMedia**
  Out-of-bounds access leading to process termination
- **CVE-2026-28886 – CoreUtils**
  Null pointer dereference causing denial-of-service
- **CVE-2026-28878 – Crash Reporter**
  Installed app enumeration (privacy issue)
- **CVE-2025-14524 – curl (Third-party)**
  Leakage of sensitive data over incorrect connection
- **CVE-2026-28876 – DeviceLink**
  Sensitive data exposure due to improper path validation
- **CVE-2026-28870 – GeoServices**
  Information leakage vulnerability
- **CVE-2026-28880 – iCloud**
  App enumeration due to permission issue
- **CVE-2026-28833 – iCloud**

Privacy exposure via installed app discovery

- **CVE-2025-64505 – ImageIO (Third-party)**
  Malicious file processing leading to app crash

Kernel Vulnerabilities (High Risk)

- **CVE-2026-28868 – Kernel**
  Kernel memory disclosure
- **CVE-2026-28867 – Kernel**
  Leakage of sensitive kernel state
- **CVE-2026-20698 – Kernel**
  Kernel memory corruption and system crash
- **CVE-2026-20687 – Kernel**
  Use-after-free allowing kernel memory write

Privilege & Sandbox Issues

- **CVE-2026-28882 – libxpc**
  App enumeration vulnerability
- **CVE-2026-20688 – Printing**
  Sandbox escape via path handling issue
- **CVE-2026-28863 – Sandbox Profiles**
  User fingerprinting
- **CVE-2026-28864 – Security**
  Unauthorized access to Keychain items

Privacy & Local Attack Surface

- **CVE-2026-28856 – Siri**
  Exposure of sensitive data on locked device
- **CVE-2026-20692 – Mail**
  Failure of privacy protections (IP/remote content leakage)

Network & Telephony

- **CVE-2026-28858 – Telephony**
  Buffer overflow leading to kernel memory corruption

WebKit Vulnerabilities (Critical – Web-based Attacks)

- **CVE-2026-20665 – WebKit**
  Content Security Policy bypass
- **CVE-2026-20643 – WebKit**
  Same Origin Policy bypass
- **CVE-2026-28871 – WebKit**
  Cross-site scripting (XSS) via malicious website
- **CVE-2026-20664 – WebKit**
  Memory handling issue leading to crash
- **CVE-2026-28857 – WebKit**
  Additional memory corruption vulnerability
- **CVE-2026-28861 – WebKit**
  Cross-origin access to restricted handlers
- **CVE-2026-28859 – WebKit**
  Sandbox escape via malicious web content
- **CVE-2026-20691 – WebKit Sandboxing**

Software Updates Details:

Name	Available for
iOS 26.4 and iPadOS 26.4	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 18.7.7 and iPadOS 18.7.7	iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation
macOS Tahoe 26.4	macOS Tahoe
macOS Sequoia 15.7.5	macOS Sequoia
macOS Sonoma 14.8.5	macOS Sonoma
tvOS 26.4	Apple TV HD and Apple TV 4K (all models)
watchOS 5.3.10	Apple Watch Series 1, Series 2, Series 3, and Series 4
watchOS 8.8.2	Apple Watch Series 3, Series 4, Series 5, Series 6, Series 7, and SE
watchOS 26.4	Apple Watch Series 6 and later
visionOS 26.4	Apple Vision Pro (all models)
Safari 26.4	macOS Sonoma and macOS Sequoia
Xcode 26.4	macOS Tahoe 26.2 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