GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

18 November 2026

Advisory 382: Apple Multiple Products WebKit Pointer Authentication Bypass Vulnerability (CVE-2024-27834).

Release Date: 11th November 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2024-27834 is an improper authentication vulnerability in WebKit, the browser engine used by Safari and all browsers on iPhone and iPad. An attacker who already has arbitrary read and write capability may be able to bypass Pointer Authentication, a hardware protection on Apple devices that blocks memory-corruption exploits. On its own it is rated CVSS 5.5 (Medium), but it is a key link in exploit chains that turn a browser bug into full code execution.

What are the systems affected?

The vulnerability affects devices and software that have not been updated since May 2024:

- iPhone and iPad before iOS and iPadOS 17.5, or before 16.7.8 on older devices
- Mac before macOS Sonoma 14.5, and Safari before 17.5 on macOS Monterey and Ventura
- Apple TV before tvOS 17.5 and Apple Watch before watchOS 10.5
- Linux applications using WebKitGTK or WPE WebKit before 2.44.2

Not affected / patched version:

- iOS and iPadOS 17.5 or 16.7.8, macOS Sonoma 14.5, Safari 17.5, tvOS 17.5, watchOS 10.5 or later
- WebKitGTK and WPE WebKit 2.44.2 or later

What does this mean?

Successful exploitation, as part of an exploit chain, may allow attackers to:

- Run code on a device after the user visits a malicious or compromised website
- Steal browser cookies, saved passwords and session tokens
- Take over email, cloud and social media accounts using stolen sessions

Mitigation process

CERTVU recommends the following:

1. Update Apple devices
Update all iPhones, iPads, Macs, Apple TVs and Apple Watches to the latest version available for each device. Any device on a version from before May 2024 should be updated now.

2. Replace devices that cannot be updated
3. Update Linux WebKit packages
4. Protect accounts

. Report suspected compromise to CERTVU at incident@cert.gov.vu.

Reference

1. https://support.apple.com/en-us/100100
2. https://www.cve.org/CVERecord?id=CVE-2024-27834
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2024-27834