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 December 2025

Advisory 116: Apple Multiple Products Use-After-Free WebKit Vulnerability

Release Date: 15th of December 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication 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 products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-43529 is a use-after-free vulnerability in WebKit, the browser engine used by **Safari** and all WebKit-based browsers on Apple platforms. A use-after-free occurs when software continues to reference memory that has already been freed, which can lead **to** memory corruption and remote code execution (RCE) when processing crafted content. This vulnerability is actively exploited in the wild.

What are the Systems affected?

The vulnerability affects Apple devices and OS components that use WebKit, including:

- **iOS** and **iPadOS** (pre-26.2/18.7.3)
- **macOS Tahoe** (pre-26.2)
- **tvOS**, **watchOS**, **visionOS** (pre-26.2)
- **Safari browser** on those platforms

In practice, this means many iPhones, iPads, Macs, Apple TVs, Apple Watches, and Vision Pro devices running older OS versions are vulnerable.

What does this mean?

How attackers exploit this vulnerability (attack vector)

An attacker crafts **malicious HTML/CSS/JavaScript** that triggers the use-after-free inside WebKit while the victim's browser renders the page. This causes memory to be corrupt in a controlled way, enabling the attacker to **execute arbitrary code** in the context of the browser process.

• **Impact:** Successfully exploited, this can lead to:

- **Remote Code Execution (RCE)** — the attacker runs code on the device as the browser user
- **Privilege misuse** if combined with other flaws
- Further compromise of the device via chained exploits

Mitigation process

CERTVU recommend:

Patch Immediately: install the security updates Apple released (these address CVE-2025-43529):

- **iOS & iPadOS:** 18.7.3, 26.2 or later
- **macOS Tahoe:** 26.2 or later
- **tvOS, watchOS, visionOS:** 26.2 or later
- **Safari:** 26.2 or later

Reference

1. https://threatprotect.qualys.com/2025/12/16/apple-warns-of-zero-day-vulnerability-exploited-in-attack-cve-2025-43529/
2. https://support.apple.com/en-us/125886
3. https://support.apple.com/en-us/125885

.