CVE-2025-24201: Out-of-Bounds Write Issue in Apple Devices

Vairav CVE Report

Date: March 12th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A severe vulnerability, identified as CVE-2025-24201, has been discovered in Apple's WebKit browser engine, affecting multiple Apple products. This out-of-bounds write issue allows maliciously crafted web content to break out of the Web Content sandbox, potentially leading to unauthorized actions such as remote code execution (RCE). Apple has acknowledged reports that this vulnerability has been exploited in "extremely sophisticated" attacks against specific targeted individuals on versions of iOS before iOS 17.2. The Common Vulnerability Scoring System (CVSS) score for this vulnerability has not yet been provided.

VULNERABILITY DETAILS

CVE-2025-24201

- **Description:** An out-of-bounds write issue exists in the WebKit component, which could be exploited through maliciously crafted web content. This flaw allows attackers to escape the Web Content sandbox, leading to unauthorized actions on the affected device.
- **Impact:** Successful exploitation of this vulnerability could result in remote code execution, allowing attackers to execute arbitrary code on the affected device. This could lead to full system compromise, data exposure, or service disruption.
- **CVSS Score:** Not yet provided.

AFFECTED VERSIONS

The following Apple products and versions are affected by this vulnerability:

- **iOS and iPadOS:** Versions before 18.3.2, affecting devices including 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).
- **macOS Sequoia:** Versions before 15.3.2.
- **Safari:** Versions before 18.3.1.
- **visionOS:** Versions before 2.3.2, affecting Apple Vision Pro devices.

EXPLOIT DETAILS

This vulnerability has been exploited in highly targeted attacks against specific individuals. Attackers can exploit this flaw by convincing users to visit maliciously crafted web content, which can then escape the Web Content sandbox and execute arbitrary code on the device. The sophistication of these attacks suggests potential involvement of advanced persistent threat (APT) actors or nation-state adversaries.

RECOMMENDED ACTIONS

Patch & Upgrade:

- **iOS and iPadOS:** Upgrade to version 18.3.2.
- **macOS Sequoia:** Upgrade to version 15.3.2.
- **Safari:** Upgrade to version 18.3.1.
- **visionOS:** Upgrade to version 2.3.2.

ADDITIONAL SECURITY MEASURES

- **Enable Lockdown Mode**: For users at higher risk, such as those in sensitive professions or regions, enabling Lockdown Mode can provide enhanced security by restricting certain device functionalities to reduce the attack surface.
- **Exercise Caution with Untrusted Links**: Avoid clicking on links or opening attachments from unknown or untrusted sources, as they may lead to malicious websites designed to exploit this vulnerability.
- **Regular Security Audits**: Organizations should conduct regular security assessments and audits to identify and mitigate potential vulnerabilities within their networks and devices.

REFERENCES

- https://support.apple.com/en-us/100100
- https://thehackernews.com/2025/03/apple-releases-patch-for-webkit-zero.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com