NATIONAL CSIRT-CY

CVE-2025-24201 **14/3/2025**

Out-of-Bounds Write Vulnerability in WebKit Leading to Sandbox Escape

Executive Summary

This vulnerability is present in WebKit's handling of out-of-bounds write operations, which allows an attacker to execute arbitrary code and escape the Web Content sandbox. This could enable an attacker to bypass security controls and execute malicious code outside of the intended environment.

Analysis

If a user visits a malicious website, the attacker could exploit the out-of-bounds write vulnerability in WebKit to modify memory outside of its allocated bounds. This could lead to arbitrary code execution and enable the attacker to escape the Web Content sandbox, gaining higher-level access to the system. The vulnerability is particularly dangerous because it has already been exploited in targeted attacks on older versions of iOS, suggesting a high risk for targeted exploitation.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/164.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-24201

Versions affected

- **iOS** – Versions prior to iOS 18.3.2
- **iPadOS** – Versions prior to iPadOS 18.3.2
- **macOS** – Versions prior to macOS Sequoia 15.3.2
- **Safari** – Versions prior to Safari 18.3.1
- **visionOS** – Versions prior to visionOS 2.3.2

Solutions

To mitigate the risks associated with CVE-2025-24201, Apple has released security updates that address the vulnerability through improved bounds checking. Users should update to the latest versions of iOS (18.3.2), iPadOS (18.3.2), macOS (Sequoia 15.3.2), Safari (18.3.1), and visionOS (2.3.2) to ensure their devices are protected.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.