Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Addresses WebKit Zero-Day Exploited in Sophisticated Attacks

Date of Publication	Admiralty Code	TA Number
March 12, 2025	A1	TA2025074

Summary

First Seen: March 11, 2025
Affected Products: Apple iOS and iPadOS, macOS Sequoia, visionOS, Safari
Impact: Apple has released a fix for a zero-day vulnerability, CVE-2025-24201, affecting the WebKit browser engine. This flaw has been actively exploited in highly sophisticated attacks, allowing threat actors to escape the Web Content sandbox using maliciously crafted web pages. The update serves as a supplementary patch to reinforce protections against an attack that was initially mitigated in iOS 17.2.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24201	Apple Multiple Products Out-of-Bounds Write Vulnerability	Apple iOS and iPadOS, macOS Sequoia, visionOS, Safari	✓	✗	✓

Vulnerability Details

#1

Apple has addressed CVE-2025-24201, a zero-day vulnerability in the WebKit browser engine. This flaw, exploited in highly sophisticated attacks, is caused by an out-of-bounds write issue that can be triggered through malicious web content. If exploited, attackers can break out of WebKit’s Web Content sandbox, potentially gaining deeper access to the system. WebKit is the browser engine behind Apple's Safari and many other apps and web browsers on macOS, iOS, Linux, and Windows.

#2 This update is especially crucial for users on or before iOS 17.2, as the vulnerability has been exploited in sophisticated attacks targeting this version. It serves as an additional fix for an attack that Apple had previously blocked. The vulnerability has been used in targeted attacks against certain individuals running older versions of iOS. The level of sophistication in these attacks suggests they were carried out by well-resourced threat actors.

#3 With this latest update, Apple has patched three actively exploited zero-day vulnerabilities this year. Alongside CVE-2025-24201, the company has also addressed **CVE-2025-24085** and **CVE-2025-24200**. To stay protected from potential attacks, users should update their devices to the latest version as soon as possible. Keeping software up to date is crucial in defending against actively exploited vulnerabilities like CVE-2025-24201.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24201	Apple iOS and iPadOS Versions before 18.3.2, Apple macOS Sequoia Versions before 15.3.2, Apple visionOS Version before 2.3.2, Apple Safari Version before 18.3.1	cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos_sequoia:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-787

Recommendations

Stay Updated: Keep your iOS and macOS devices up to date to patch the CVE-2025-24201 zero-day vulnerability and protect against potential threats.

Choose a Secure Browser: Use browsers with strong security features, as WebKit flaws can impact Safari and other Apple-based browsers.

Turn on Automatic Updates: Ensure automatic updates are enabled on your Apple devices so you receive security patches as soon as they become available.

Strengthen Web Security: Use trusted security software or browser extensions to detect and block malicious content and restrict unnecessary web permissions to reduce potential attack risks.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0007** Discovery	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1497** Virtualization/Sandbox Evasion	**T1190** Exploit Public-Facing Application	

Patch Details

To address the CVE-2025-24201 vulnerability upgrade to the latest iOS and macOS versions immediately.

Links:
For visionOS Upgrade to Version 2.3.2
https://support.apple.com/en-us/118481

For iOS Upgrade to Version 18.3.2
https://support.apple.com/en-us/118575

For iPadOS Upgrade to Version 18.3.2
https://support.apple.com/en-us/118575

For macOS Sequoia Upgrade to Version 15.3.2
https://support.apple.com/en-us/108382

For Safari Upgrade to Version 18.3.1
https://support.apple.com/en-us/122285

References

https://support.apple.com/en-us/122281

https://support.apple.com/en-us/122283

https://support.apple.com/en-us/122284

https://support.apple.com/en-us/122285

https://hivepro.com/threat-advisory/apple-fixes-zero-day-exploit-that-bypasses-usb-restricted-mode/

https://hivepro.com/threat-advisory/Apple-Tackles-First-Zero-Day-of-2025-Actively-Exploited-in-the-Wild/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

March 12, 2025 • 4:45 AM

More at www.hivepro.com