

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Apple Addresses Actively Exploited Zero-Day Flaws in macOS and iOS

Date of Publication

November 20, 2024

Admiralty Code

A1

TA Number

TA2024437







Summary

First Seen: November 2024

Affected Products: macOS, iOS, visionOS, iPadOS, and Safari

Impact: Apple has addressed two actively exploited zero-day vulnerabilities, CVE-2024-44308 and CVE-2024-44309, affecting Intel-based Mac systems. These flaws were discovered in the macOS Sequoia JavaScriptCore (CVE-2024-44308) and WebKit (CVE-2024-44309) components, posing significant security risks. Users are strongly encouraged to update their devices immediately to safeguard against potential exploitation.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-44308	Apple Multiple Products Code Execution Vulnerability	macOS, iOS, visionOS, iPadOS and Safari			
CVE-2024-44309	Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability	macOS, iOS, visionOS, iPadOS and Safari			

Vulnerability Details

#1

Apple has issued critical security updates for macOS and iOS to address two actively exploited zero-day vulnerabilities, CVE-2024-44308 and CVE-2024-44309, found in the JavaScriptCore and WebKit components of macOS. CVE-2024-44308 stems from insufficient validation of user-supplied input in the JavaScriptCore component. An attacker could exploit this vulnerability by tricking a victim into visiting a maliciously crafted webpage, enabling arbitrary code execution on the targeted system.

#2

CVE-2024-44309 a cookie management flaw within WebKit, allowing attackers to carry out cross-site scripting (XSS) attacks through maliciously crafted web content. This vulnerability could lead to unauthorized script execution on trusted websites, compromising user data and web session integrity.

#3

Both vulnerabilities are being actively exploited in real-world attacks, making it critical for macOS and iOS users to apply the latest updates immediately. These incidents underscore the importance of timely patching and vigilance in maintaining secure systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-44308	Safari Version Prior to 18.1, macOS Version Prior to 15.1, iOS and iPadOS Version Prior to 18.1, visionOS Version Prior to 2.1	cpe:2.3:a:apple:visionos:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*	CWE-20
CVE-2024-44309	Safari Version Prior to 18.1, macOS Version Prior to 15.1, iOS and iPadOS Version Prior to 18.1, visionOS Version Prior to 2.1	cpe:2.3:a:apple:visionos:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:** cpe:2.3:a:apple:ios:*:*:*:*:*:*	CWE-79

Recommendations



Apply Patches: Users are strongly advised to update their macOS and iOS devices to the latest versions to patch CVE-2024-44308 and CVE-2024-44309. Ensuring that all devices are running the latest security updates is crucial to protect against these active threats.



Regular Updates and Monitoring: Ensure all macOS and iOS devices are updated promptly with the latest security patches to protect against vulnerabilities like CVE-2024-44308 and CVE-2024-44309. Establish a routine schedule for monitoring and applying updates across all devices to mitigate risks from newly discovered threats.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0006</u> Credential Access
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1059</u> Command and Scripting Interpreter
<u>T1059.007</u> JavaScript	<u>T1189</u> Drive-by Compromise	<u>T1606</u> Forge Web Credentials	<u>T1606.001</u> Web Cookies

Patch Details

To address the zero-day vulnerabilities CVE-2024-44308 and CVE-2024-44309, Apple has released security updates in the following versions. It is strongly recommended that users update to these versions immediately to mitigate the risks.

Fixed Versions:

Safari 18.1.1

iOS 17.7.2 and iPadOS 17.7.2

macOS Sequoia 15.1.1

iOS 18.1.1 and iPadOS 18.1.1

visionOS 2.1.1

Links: <https://support.apple.com/en-us/118575>

<https://support.apple.com/en-us/118481>

<https://support.apple.com/en-us/108382>

References

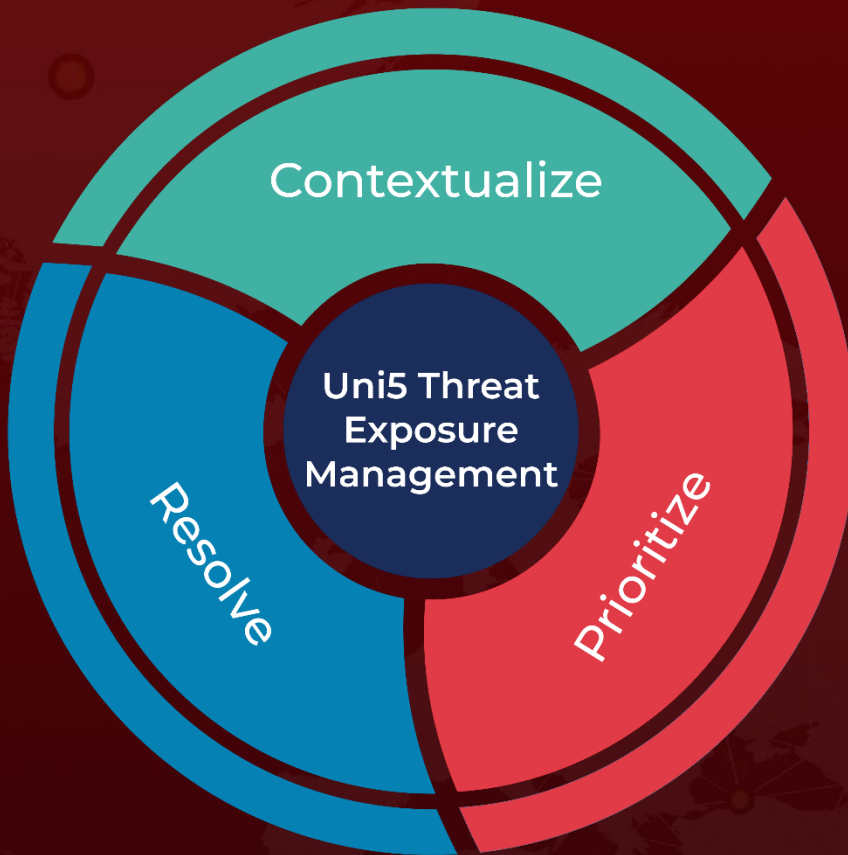
<https://support.apple.com/en-us/121753>

<https://vulnera.com/newswire/apple-patches-two-zero-day-vulnerabilities-in-intel-based-macs/>

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.



REPORT GENERATED ON

November 20, 2024 • 5:50 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com