Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Fixes First Actively Exploited Zero-day of 2024

Date of Publication	Admiralty Code	TA Number
January 23, 2024	A1	TA2024027

Summary

First Seen: January 22, 2024
Affected Platform: iPhone, iPad, tvOS, Safari and Mac running macOS Monterey, Ventura, Sonoma
Impact: The CVE-2024-23222 vulnerability in Apple's WebKit is actively being exploited, as the processing of maliciously crafted web content may result in arbitrary code execution, posing a severe threat to the security and control of affected tvOS, iPhones, iPads, and macOS. Immediate updating is crucial to mitigate potential exploitation risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-23222	Apple Multiple Products Type Confusion Vulnerability	Apple Multiple Products	✓	✓	✓

Vulnerability Details

#1

Apple has released urgent security updates to address a critical zero-day vulnerability, tracked as CVE-2024-23222, actively exploited by attackers. This flaw resides in WebKit, the engine powering Safari and other web-based apps on tvOS, iPhones, iPads, and macOS. It is a type confusion bug, triggered by processing malicious web content, could result in arbitrary code execution, giving attackers remote control over affected devices.

#2

The updates cover various devices and operating systems, marking the first actively exploited zero-day patched by Apple this year. Apple acknowledged the exploitation report but provided no details on the attacks or threat actors. Additionally, Apple backported fixes for CVE-2023-42916 and CVE-2023-42917 to older devices.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-23222	iPhone, iPad, tvOS, Safari and Mac running macOS Monterey, Ventura, Sonoma	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:tvos:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Update Immediately: Apply the latest security updates provided by Apple for affected devices, including iOS, iPadOS, macOS, and Safari, to patch the identified vulnerability.

Regularly Update Software: Keep all software, including browsers and applications, up to date to address potential vulnerabilities.

User Vigilance: Exercise caution when interacting with web content, especially if it appears suspicious or is from unfamiliar sources. Be mindful of potential phishing attempts or malicious websites that could exploit the identified flaws.

Review and Adjust Browser Security Settings: Evaluate and adjust browser security settings on Apple devices to ensure an optimal balance between usability and security. Consider disabling unnecessary features that may expose devices to potential risks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	T1588.006 Vulnerabilities	T1588 Obtain Capabilities
T1203 Exploitation for Client Execution	T1588.005 Exploits		

Patch Details

To mitigate the CVE-2024-23222 vulnerability in Apple's WebKit, users should immediately apply tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3 or later versions.

Links:
https://support.apple.com/en-us/HT214055

https://support.apple.com/en-us/HT214056

https://support.apple.com/en-us/HT214057

https://support.apple.com/en-us/HT214058

https://support.apple.com/en-us/HT214059

https://support.apple.com/en-us/HT214060

https://support.apple.com/en-us/HT214061

https://support.apple.com/en-us/HT214063

References

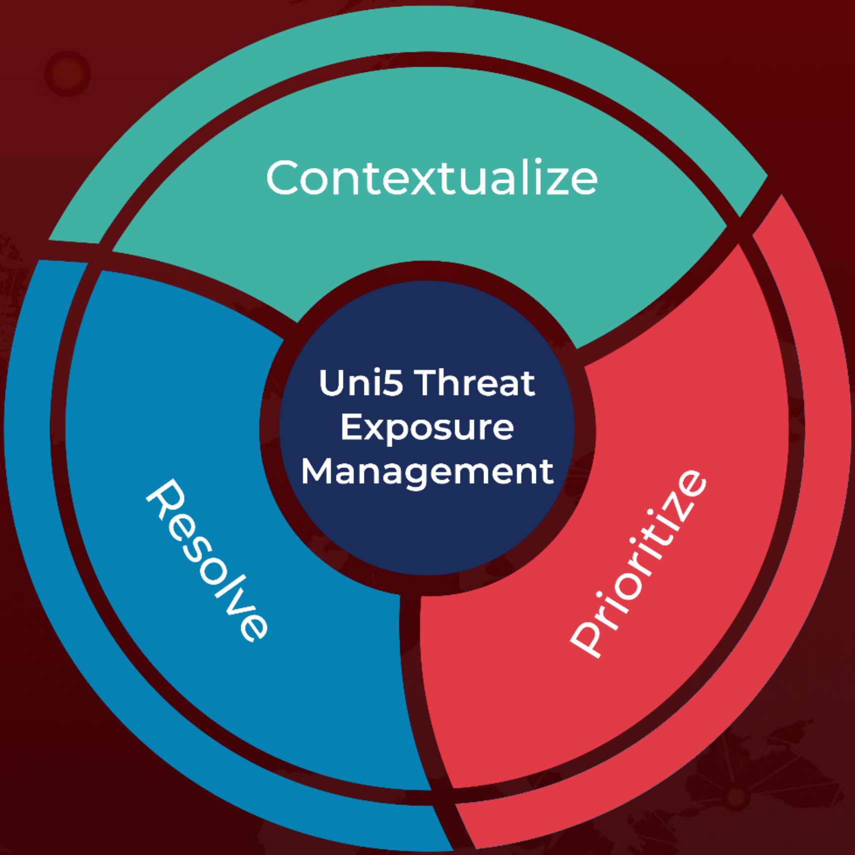
https://thehackernews.com/2024/01/apple-issues-patch-for-critical-zero.html

https://www.hivepro.com/threat-advisory/apples-timely-response-to-actively-exploited-zero-days/

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

January 23, 2024 • 3:30 AM

More at www.hivepro.com