Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple WebKit Zero-Days Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
December 17, 2025	A1	TA2025381

Summary

First Seen: December 2025
Affected Products: Apple WebKit, Safari, all WebKit-based browsers
Affected Platforms: iOS, iPadOS, macOS, watchOS, tvOS, visionOS
Impact: Apple has released emergency security updates to address two actively exploited zero-day vulnerabilities in its WebKit browser engine, tracked as CVE-2025-43529 and CVE-2025-14174. These flaws affect Safari and all browsers on iOS and iPadOS, as well as WebKit on macOS and other Apple platforms, and can be triggered simply by visiting a maliciously crafted webpage. Apple confirmed the vulnerabilities were used in highly sophisticated, targeted attacks, potentially enabling remote code execution. Given the confirmed in-the-wild exploitation and broad platform impact, immediate patching is critical to reduce the risk of device compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-43529	Apple Multiple Products Use-After-Free WebKit Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2025-14174	Google Chromium Out of Bounds Memory Access Vulnerability	Apple Multiple Products	✓	✓	✓

Vulnerability Details

#1

Apple has released emergency security updates across its entire platform stack to remediate two actively exploited zero-day vulnerabilities in its WebKit browser engine, tracked as CVE-2025-43529 and CVE-2025-14174. These flaws affect WebKit, the rendering engine behind Safari and all browsers on iOS and iPadOS, meaning that virtually any web content rendered in these environment could trigger the vulnerabilities. Apple confirmed that at least one of the bugs was used in highly sophisticated real-world attacks against specific targeted individuals before the patches were available, underscoring the immediate risk posed by both issues.

#2

CVE-2025-43529 is a use-after-free vulnerability in WebKit. A use-after-free occurs when a program continues to use memory after it has been released, potentially allowing an attacker to manipulate memory state and execute arbitrary code when crafted web content is processed. This kind of flaw is often a key component in remote exploitation chains. CVE-2025-14174, on the other hand, is a memory corruption issue tied to the ANGLE graphics abstraction layer used in WebKit, originally observed and patched by Google in Chrome before being disclosed as this shared CVE. Both vulnerabilities can be triggered when the browser loads maliciously crafted web content, with no additional app installation required.

#3

Because WebKit is mandatory for all third-party browsers on iOS and iPadOS, these flaws extend beyond Safari to any browser on those platforms that relies on WebKit. They also affected WebKit on macOS and other Apple operating systems such as tvOS, watchOS, and visionOS. The ANGLE-related memory corruption aspect of CVE-2025-14174, shared with Chrome's implementation, highlights that the underlying issue has cross-browser implications beyond just Apple's stack.

#4

To address these high-severity issues, Apple released patches in iOS/iPadOS 26.2 and 18.7.3 (for older devices), macOS Tahoe 26.2, Safari 26.2, and updated versions of tvOS, watchOS, and visionOS. Users and administrators are strongly urged to apply these updates immediately because unpatched devices remain vulnerable to code execution and compromise via crafted web pages.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-43529	iOS / iPadOS: versions earlier than 26.2 and 18.7.3 macOS: versions earlier than Tahoe 26.2 Safari: versions earlier than 26.2 tvOS: versions earlier than 26.2 watchOS: versions earlier than 26.2 visionOS: versions earlier than 26.2 Google Chrome (macOS): versions earlier than 143.0.7499.110 Microsoft Edge (macOS): versions prior to 143.0.3650.80	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-14174			CWE-119 CWE-787

Recommendations

Apply Security Updates Immediately: Ensure all Apple devices are updated to the latest patched versions, including iOS/iPadOS 26.2 (or 18.7.3 for older devices), macOS Tahoe 26.2, Safari 26.2, and corresponding updates for watchOS, tvOS, and visionOS. Unpatched systems remain vulnerable to remote exploitation via web content.

Update Third-Party Browsers on macOS: Update Google Chrome to version 143.0.7499.110 or later and Microsoft Edge to version 143.0.3650.80, as CVE-2025-14174 affects the shared ANGLE graphics engine used across multiple browsers.

Enhance Monitoring and Detection: Monitor endpoints and mobile device logs for abnormal browser crashes, WebKit or GPU process failures, and unusual WebGL activity that may indicate exploitation attempts.

Reduce Exposure to Malicious Web Content: Enforce web filtering where possible, caution users against clicking untrusted links, and consider enabling Apple Lockdown Mode for users at elevated risk until patching is fully completed.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0004 Privilege Escalation	TA0006 Credential Access	T1203 Exploitation for Client Execution	T1555 Credentials from Password Stores
T1059.007 JavaScript	T1059 Command and Scripting Interpreter	T1211 Exploitation for Defense Evasion	T1204 User Execution
T1068 Exploitation for Privilege Escalation	T1588.005 Exploits	T1588.006 Vulnerabilities	T1588 Obtain Capabilities
T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application	T1204.001 Malicious Link	

Patch Details

Apply updates immediately to all affected devices and browsers to mitigate active exploitation.

iOS / iPadOS: 26.2 / 18.7.3
macOS Tahoe: 26.2
Safari: 26.2
tvOS / watchOS / visionOS: 26.2
Chrome (macOS): 143.0.7499.110 or later
Microsoft Edge (macOS): 143.0.3650.80 or later

Links:
https://support.apple.com/en-us/100100
https://support.apple.com/en-us/125892,
https://support.apple.com/en-us/125886,
https://support.apple.com/en-us/125885,
https://support.apple.com/en-us/125884,

https://support.apple.com/en-us/125892,
https://support.apple.com/en-us/125889,
https://support.apple.com/en-us/125890,
https://support.apple.com/en-us/125891,
https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html,
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-14174

References

https://threatprotect.qualys.com/2025/12/16/apple-warns-of-zero-day-vulnerability-exploited-in-attack-cve-2025-43529/

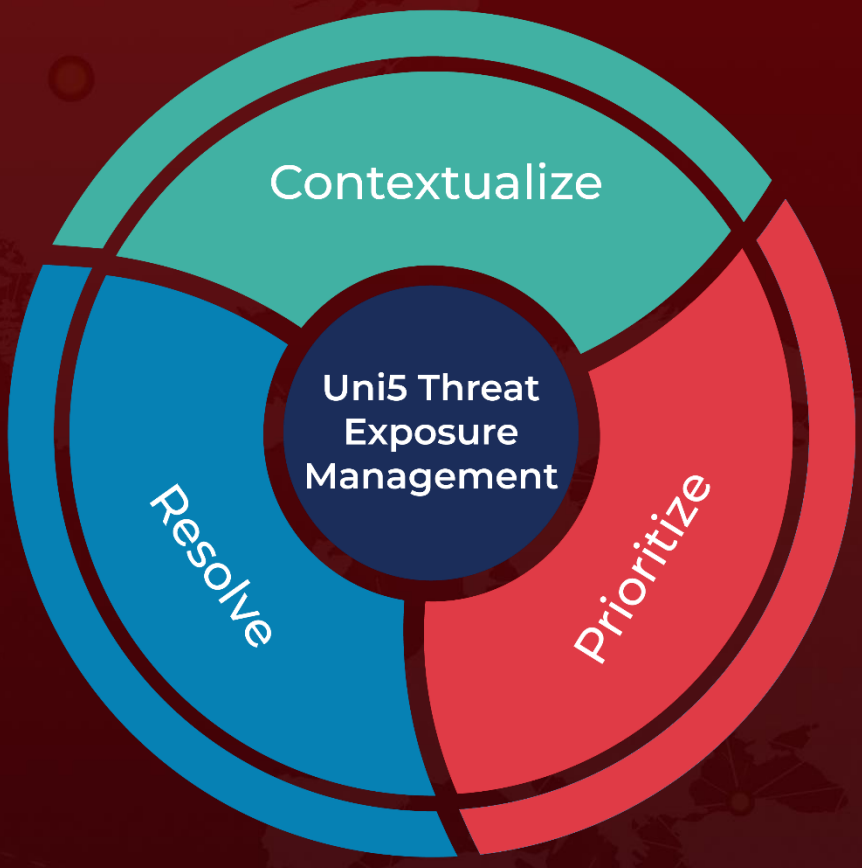
https://support.apple.com/en-us/100100

https://hivepro.com/threat-advisory/google-chrome-zero-day-exploited-in-angle-graphics-engine/

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

December 17, 2025 • 9:00 AM

More at www.hivepro.com