Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Tackles First Zero-Day of 2025, Actively Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
January 28, 2025	A1	TA2025023

Summary

First Seen: January 27, 2025
Affected Products: Apple Multiple Products
Impact: Apple has swiftly released emergency security updates for iOS, iPadOS, macOS, tvOS, watchOS, and visionOS to patch a critical zero-day vulnerability, CVE-2025-24085, which is actively being exploited. This serious flaw enables malicious apps to potentially elevate their privileges on vulnerable devices. In addition to this, Apple has also addressed several other vulnerabilities across its product line, which could lead to denial-of-service (DoS) attacks, arbitrary code execution, and privilege escalation.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24085	Apple Multiple Products Use After Free Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2025-24131	Apple Multiple Products Denial-of-service Vulnerability	Apple Multiple Products	✗	✗	✓
CVE-2025-24177	Apple Multiple Products Denial-of-service Vulnerability	Apple Multiple Products	✗	✗	✓
CVE-2025-24107	Apple Multiple Products Privilege Escalation Vulnerability	Apple Multiple Products	✗	✗	✓
CVE-2025-24159	Apple Multiple Products Arbitrary Code Execution Vulnerability	Apple Multiple Products	✗	✗	✓
CVE-2025-24158	Apple Multiple Products Denial-of-service Vulnerability	Apple Multiple Products	✗	✗	✓

Vulnerability Details

#1 Apple has released critical software updates to address multiple security vulnerabilities across its devices, including a zero-day flaw that is actively being exploited. The most concerning of these vulnerabilities, tracked as CVE-2025-24085, is a use-after-free bug within the Core Media component. This framework is a crucial part of the media pipeline, handling media tasks for AVFoundation and other high-level media frameworks in Apple's ecosystem. The flaw allows malicious apps, already installed on a device, to escalate their privileges, which significantly increases the security risks.

#2 In addition to this zero-day issue, Apple has patched several other vulnerabilities that could have serious consequences for device security. CVE-2025-24131 a memory handling issue that could potentially allow a privileged attacker to launch a denial-of-service (DoS) attack. CVE-2025-24177 a null pointer dereference flaw, which could enable remote attackers to trigger a DoS.

#3 CVE-2025-24107 is a permissions issue that allows local applications to escalate privileges and execute arbitrary code with root access. CVE-2025-24159 a validation flaw that could allow apps to execute arbitrary code with kernel-level privileges. Finally, CVE-2025-24158 a memory handling flaw that could cause a DoS attack when processing web content.

#4 Although the specifics of how these vulnerabilities were exploited, who is behind the attacks, and the targeted devices are still unclear, CVE-2025-24085 has been confirmed to be actively exploited. Apple strongly encourages users to promptly install the latest updates to safeguard their devices from these ongoing security threats.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24085	Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24131	Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-119
CVE-2025-24177	Apple macOS Version affected before 15.3, iOS and iPadOS Version affected before 18.3	cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-476
CVE-2025-24107	Apple tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-264
CVE-2025-24159	Apple macOS Version affected before 14.7, visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, iPadOS Version affected before 17.7, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-264
CVE-2025-24158	Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3, Safari Version affected before 18.3	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* 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-119

Recommendations

Apply Patch: It's crucial for users to install Apple's latest security patches. This is especially important for addressing the CVE-2025-24085 zero-day vulnerability, which is currently being actively exploited. Keeping your devices up-to-date is the best way to protect them from emerging threats.

Limit App Permissions: Carefully review and restrict app permissions, ensuring that apps only have access to what they truly need. It's also important to avoid installing apps from untrusted sources, as these could pose significant security risks.

Enable Multi-Factor Authentication (MFA): Whenever possible, activate multi-factor authentication (MFA) on your accounts and services. MFA adds an extra layer of security, making it more difficult for attackers to gain unauthorized access, even if they exploit vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0040** Impact
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation
T1499 Endpoint Denial of Service			

Patch Details

Promptly update to the latest version of Apple Products, these versions includes the necessary patch to address the vulnerabilities.

iOS 18.3
iPadOS 18.3
macOS Sequoia 15.3
watchOS 11.3
visionOS 2.3
tvOS 18.3

Links:
https://support.apple.com/en-us/118575
https://support.apple.com/en-us/108382
https://support.apple.com/en-us/108926
https://support.apple.com/en-us/108414

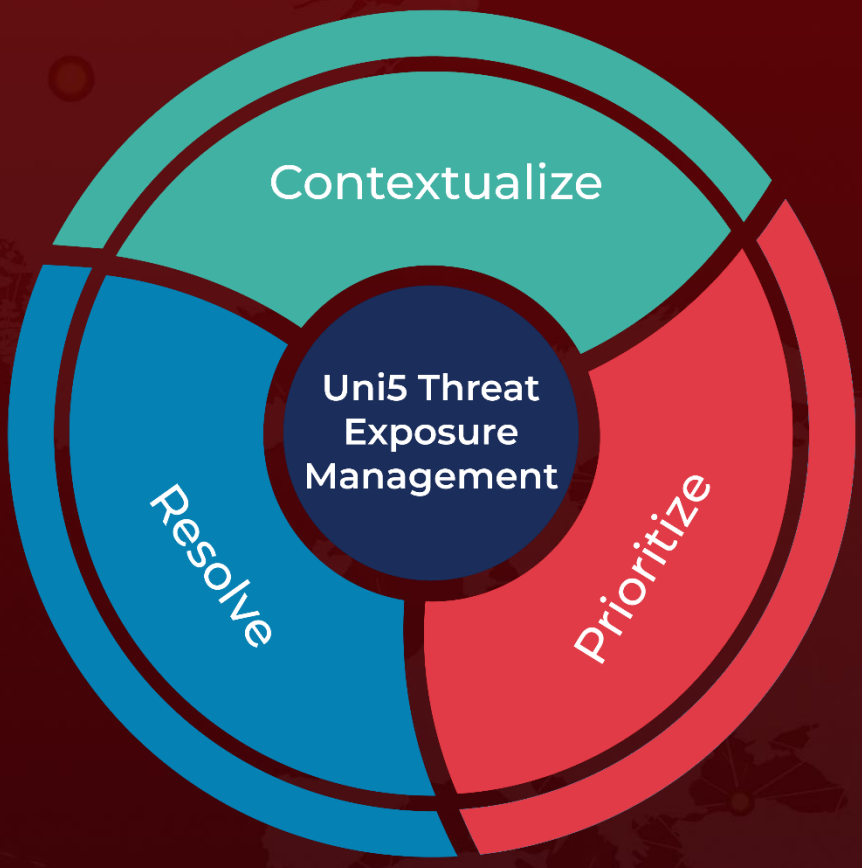
References

https://support.apple.com/en-us/122066

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 28, 2025 • 4:50 AM

More at www.hivepro.com