Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CoreAudio and RPAC Cracked: Apple Patches Active Zero-Day Threats

Date of Publication	Admiralty Code	TA Number
April 17, 2025	A1	TA2025118

Summary

First Seen: April 16, 2025
Affected Products: macOS, iOS, tvOS, iPadOS, and visionOS
Impact: Apple has released security updates to fix two zero-day vulnerabilities, tracked as CVE-2025-31200 and CVE-2025-31201 that were exploited in a highly targeted and sophisticated attack. These flaws affect a wide range of Apple devices, including iPhones, Macs, iPads, Apple TVs, and Vision Pro. The flaws could allow attackers to run harmful code or bypass critical security protections. To stay protected, make sure you update all your Apple devices as soon as possible.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-31200	Apple Multiple Products Memory Corruption Vulnerability	macOS, iOS, tvOS, iPadOS, and visionOS	✓	✓	✓
CVE-2025-31201	Apple Multiple Products Arbitrary Read and Write Vulnerability	macOS, iOS, tvOS, iPadOS, and visionOS	✓	✓	✓

Vulnerability Details

#1

Apple has patched two zero-day vulnerabilities that were actively exploited in highly sophisticated attacks targeting specific individuals. These flaws affect a wide range of Apple platforms, including macOS, iOS, iPadOS, tvOS, and even visionOS.

#2 The first flaw, tracked as CVE-2025-31200, is a memory corruption issue within CoreAudio. By processing a maliciously crafted audio stream, attackers could execute arbitrary code on a victim's device. Apple has fixed this by implementing improved bounds checking. This vulnerability was used in an attack aimed at selected iOS users.

#3 The second flaw, CVE-2025-31201, involves Apple’s RPAC (Return Pointer Authentication Code) and is potentially more severe. It allowed attackers with arbitrary read and write capabilities to bypass Pointer Authentication a critical security mechanism designed to protect against memory corruption by verifying that pointers haven’t been tampered with. Apple mitigated this flaw by removing the vulnerable code entirely.

#4 Given that these vulnerabilities are being actively used in targeted attacks, Apple urges all users to update their devices immediately. Staying on the latest version is essential to defend against these kinds of stealthy, high-level exploits.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-31200	macOS Prior to Version 15.4.1 iOS and iPadOS Prior to Version 18.4.1 tvOS Prior to Version 18.4.1 visionOS Prior to Version 2.4.1	cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-787
CVE-2025-31201			CWE-287

Recommendations

Update Your Apple Devices Right Away: Make sure to install the latest updates on your Mac, iPhone, iPad, Apple TV, or Vision Pro as soon as possible. Apple has fixed serious security flaws that hackers are already using in attacks. Updating now helps keep your devices safe.

Turn On Automatic Updates: Enable automatic updates for all your Apple devices so you get the latest security fixes as soon as they're available. It's an easy way to stay protected without having to think about it.

Be Cautious with Unknown Media Files: Try not to open audio or video files from sources you don't recognize or trust. One of the vulnerabilities (CVE-2025-31200) can be exploited just by playing a malicious media file, so it's best to stay cautious.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1566** Phishing
T1203 Exploitation for Client Execution	**T1068** Exploitation for Privilege Escalation		

Patch Details

To address the vulnerabilities upgrade to the latest iOS and macOS versions immediately.

Links:
For macOS Upgrade to Version 15.4.1
https://support.apple.com/en-us/108382

For iOS and iPadOS Upgrade to Version 18.4.1
https://support.apple.com/en-us/118575

For tvOS Upgrade to Version 18.4.1
https://support.apple.com/en-us/108414

For visionOS Upgrade to Version 2.4.1
https://support.apple.com/en-us/118481

References

https://support.apple.com/en-us/122400

https://support.apple.com/en-us/122282

https://support.apple.com/en-us/122401

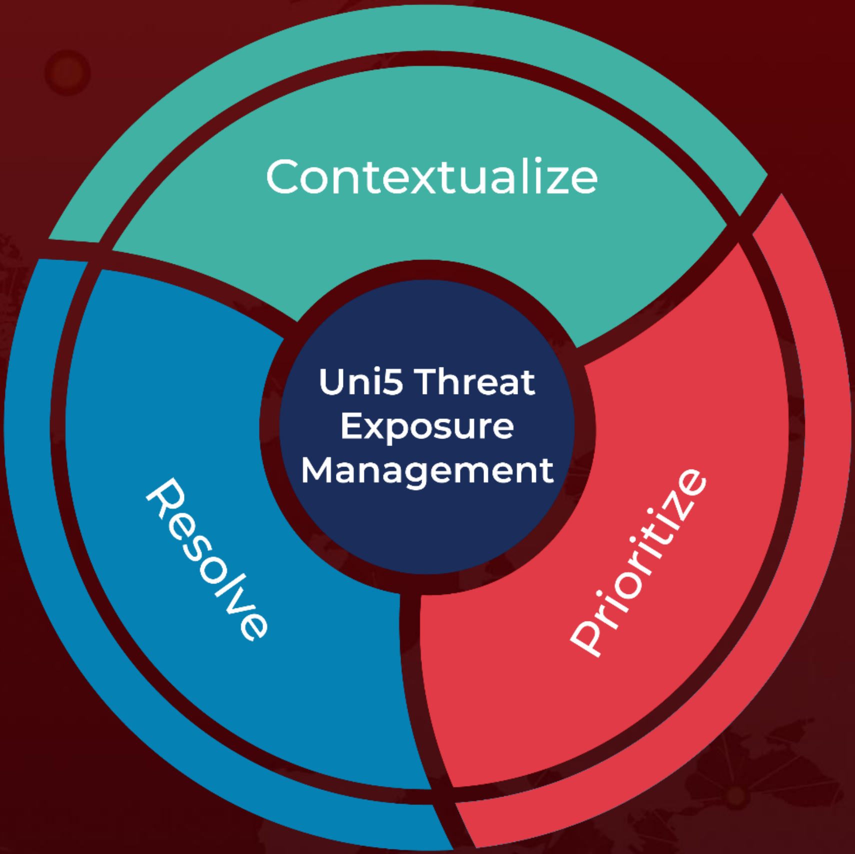
https://support.apple.com/en-us/122402

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

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

April 17, 2025 • 5:10 AM

More at www.hivepro.com