NATIONAL CSIRT-CY

**CVE-2025-31200** **19/04/2025**

# Apple's CoreAudio - Processing an audio stream in a maliciously crafted media file may result in code execution

## Executive Summary

A memory corruption issue was addressed with improved bounds checking. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. Processing an audio stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS.

## Analysis

CVE-2025-31200 affects CoreAudio, an API Apple devices use for processing audio. The memory corruption vulnerability can be triggered with a maliciously crafted media file: when the audio stream in it is processed, it allows attackers to execute malicious code.

## Common Weakness Enumeration

https://www.cve.org/CVERecord?id=CVE-2025-31200

## Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-31200

## Affected Versions

- **visionOS**: versions before **2.4**
- **iOS and iPadOS**: versions before **18.4**
- **tvOS**: versions before **18.4**
- **macOS**: versions before **15.4**

## Solutions

- **visionOS**: update to version **2.4.1**
- **iOS and iPadOS**: update to version **18.4.1**
- **tvOS**: update to version **18.4.1**
- **macOS**: update to version **15.4.1**

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

## Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.