CVE-2025-31200

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-31200
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-16 19:15:54 UTC
Updated	2026-04-02 19:19:46 UTC
Description	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in iOS 18.4.1 and iPadOS 18

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.021050000 probability, percentile 0.840320000 (date 2026-04-02)

CISA KEV: Listed on 2025-04-17; due 2025-05-08; ransomware use Unknown

Problem Types: CWE-787 | CWE-119 | 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 versions of iOS released before iOS 18.4.1. | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Apple
Product	Multiple Products
Name	Apple Multiple Products Memory Corruption Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://support.apple.com/en-us/122282 ; https://support.apple.com/en-us/122400 ; https://support.apple.com/en-us/122401 ; https://support.apple.com/en-us/122402 ; https://nvd.nist.gov/vuln/detail/CVE-2025-31200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Visionos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apple	IOS And IPadOS	affected 18.4.1 custom	Not specified
CNA	Apple	MacOS	affected 15.4.1 custom	Not specified
CNA	Apple	TvOS	affected 18.4.1 custom	Not specified
CNA	Apple	VisionOS	affected 2.4.1 custom	Not specified
CNA	Apple	WatchOS	affected 11.5 custom	Not specified

References

Reference	Source	Link
seclists.org/fulldisclosure/2025/Jun/14	af854a3a-2127-422b-91ae-364da2661108	seclists.or
seclists.org/fulldisclosure/2025/May/10	af854a3a-2127-422b-91ae-364da2661108	seclists.or
seclists.org/fulldisclosure/2025/Oct/4	af854a3a-2127-422b-91ae-364da2661108	seclists.or
support.apple.com/en-us/122722	product-security@apple.com	support.ap
news.ycombinator.com/item	af854a3a-2127-422b-91ae-364da2661108	news.ycor
support.apple.com/en-us/122402	product-security@apple.com	support.ap
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.
github.com/JGoyd/iOS-Attack-Chain-CVE-2025-31200-CVE-2025-31201/blob/mai...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.cor
support.apple.com/en-us/122400	product-security@apple.com	support.ap
support.apple.com/en-us/122282	product-security@apple.com	support.ap
support.apple.com/en-us/122401	product-security@apple.com	support.ap
seclists.org/fulldisclosure/2025/Apr/26	af854a3a-2127-422b-91ae-364da2661108	seclists.or
blog.noahhw.dev/posts/cve-2025-31200	af854a3a-2127-422b-91ae-364da2661108	blog.noah
seclists.org/fulldisclosure/2025/Oct/0	af854a3a-2127-422b-91ae-364da2661108	seclists.or
github.com/cisagov/vulnrichment/issues/200	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.cor
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.