



# CVE-2026-39869

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2026-39869
<b>State</b>	PUBLISHED
<b>Assigner</b>	apple
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-11 21:18:59 UTC
<b>Updated</b>	2026-05-12 19:16:31 UTC
<b>Description</b>	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 a

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from ADP

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

**Problem Types:** CWE-120 | Processing an audio stream in a maliciously crafted media file may terminate the process | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apple	IOS And iPadOS	affected 18.7.9 custom	Not specified
CNA	Apple	IOS And iPadOS	affected 26.5 custom	Not specified
CNA	Apple	MacOS	affected 14.8.7 custom	Not specified
CNA	Apple	MacOS	affected 15.7.7 custom	Not specified
CNA	Apple	MacOS	affected 26.5 custom	Not specified
CNA	Apple	TvOS	affected 26.5 custom	Not specified
CNA	Apple	VisionOS	affected 26.5 custom	Not specified
CNA	Apple	WatchOS	affected 26.5 custom	Not specified

### References

Reference	Source	Link	Tags
support.apple.com/en-us/127111	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127118	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127115	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127120	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127117	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127116	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127119	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/127110	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)