



# CVE-2024-27873

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

## Summary

<b>CVE</b>	CVE-2024-27873
<b>State</b>	PUBLISHED
<b>Assigner</b>	apple
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-07-29 23:15:10 UTC
<b>Updated</b>	2026-04-02 19:17:36 UTC
<b>Description</b>	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 16.7.9 and iPadOS 16.7.9

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-787 | Processing a maliciously crafted video file may lead to unexpected app termination | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apple	IOS And IPadOS	affected 16.7.9 custom	Not specified
CNA	Apple	IOS And IPadOS	affected 17.6 custom	Not specified
CNA	Apple	MacOS	affected 12.7.6 custom	Not specified
CNA	Apple	MacOS	affected 13.6.8 custom	Not specified
CNA	Apple	MacOS	affected 14.6 custom	Not specified

### References

Reference	Source	Link	Tags
support.apple.com/en-us/120912	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/HT214116	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
support.apple.com/en-us/120909	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/120910	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
seclists.org/fulldisclosure/2024/Jul/16	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third Party Advisory
support.apple.com/en-us/HT214117	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
support.apple.com/kb/HT214120	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	
seclists.org/fulldisclosure/2024/Jul/17	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third Party Advisory
support.apple.com/kb/HT214118	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/kb/HT214117	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/HT214119	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
support.apple.com/en-us/HT214120	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
seclists.org/fulldisclosure/2024/Jul/20	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third Party Advisory
seclists.org/fulldisclosure/2024/Jul/18	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third Party Advisory
support.apple.com/kb/HT214119	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/HT214118	af854a3a-2127-422b-91ae-364da2661108	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
support.apple.com/en-us/120911	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	

seclists.org/fulldisclosure/2024/Jul/19	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third Party Advisory
support.apple.com/en-us/120908	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.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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