



CVE-2025-24085

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

Summary

CVE	CVE-2025-24085
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-27 22:15:14 UTC
Updated	2026-04-03 11:44:05 UTC
Description	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.3 and iPadOS 18.3

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from nvd@nist.gov

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

EPSS: 0.139250000 probability, percentile 0.943370000 (date 2026-04-21)

CISA KEV: Listed on 2025-01-29; due 2025-02-19; ransomware use Unknown

Problem Types: CWE-416 | A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2. | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	ADP	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

CISA Known Exploited Vulnerability

Vendor	Apple
Product	Multiple Products
Name	Apple Multiple Products Use-After-Free Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://support.apple.com/en-us/122066 ; https://support.apple.com/en-us/122068 ; https://support.apple.com/en-us/122071 ; https://support.apple.com/en-us/122072 ; https://support.apple.com/en-us/122073 ; https://nvd.nist.gov/vuln/detail/CVE-2025-24085

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 18.3 custom	Not specified
CNA	Apple	iPadOS	affected 17.7.6 custom	Not specified
CNA	Apple	MacOS	affected 13.7.5 custom	Not specified
CNA	Apple	MacOS	affected 14.7.5 custom	Not specified
CNA	Apple	MacOS	affected 15.3 custom	Not specified
CNA	Apple	TvOS	affected 18.3 custom	Not specified
CNA	Apple	VisionOS	affected 2.3 custom	Not specified
CNA	Apple	WatchOS	affected 11.3 custom	Not specified

References

Reference	Source	Link
seclists.org/fulldisclosure/2025/Jun/19	af854a3a-2127-422b-91ae-364da2661108	seclists.org
support.apple.com/en-us/122072	product-security@apple.com	support.apple.com
seclists.org/fulldisclosure/2025/Apr/10	af854a3a-2127-422b-91ae-364da2661108	seclists.org

seclists.org/fulldisclosure/2025/Apr/10	af854a3a-2127-422b-91ae-364da2661108	seclists.org
seclists.org/fulldisclosure/2025/Jan/19	af854a3a-2127-422b-91ae-364da2661108	seclists.org
support.apple.com/en-us/122375	product-security@apple.com	support.apple.com
support.apple.com/en-us/122066	product-security@apple.com	support.apple.com
seclists.org/fulldisclosure/2025/Apr/5	af854a3a-2127-422b-91ae-364da2661108	seclists.org
seclists.org/fulldisclosure/2025/Apr/9	af854a3a-2127-422b-91ae-364da2661108	seclists.org
github.com/cisagov/vulnrichment/issues/194	af854a3a-2127-422b-91ae-364da2661108	github.com
seclists.org/fulldisclosure/2025/Jan/15	af854a3a-2127-422b-91ae-364da2661108	seclists.org
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
seclists.org/fulldisclosure/2025/Oct/1	af854a3a-2127-422b-91ae-364da2661108	seclists.org
github.com/JGoyd/Glass-Cage-iOS18-CVE-2025-24085-CVE-2025-24201	af854a3a-2127-422b-91ae-364da2661108	github.com
seclists.org/fulldisclosure/2025/Jan/13	af854a3a-2127-422b-91ae-364da2661108	seclists.org
seclists.org/fulldisclosure/2025/Oct/31	af854a3a-2127-422b-91ae-364da2661108	seclists.org
support.apple.com/en-us/122372	product-security@apple.com	support.apple.com
seclists.org/fulldisclosure/2025/Oct/23	af854a3a-2127-422b-91ae-364da2661108	seclists.org
seclists.org/fulldisclosure/2025/Oct/30	af854a3a-2127-422b-91ae-364da2661108	seclists.org
support.apple.com/en-us/122374	product-security@apple.com	support.apple.com
support.apple.com/en-us/122071	product-security@apple.com	support.apple.com
support.apple.com/en-us/122068	product-security@apple.com	support.apple.com
support.apple.com/en-us/122073	product-security@apple.com	support.apple.com
seclists.org/fulldisclosure/2025/Jan/12	af854a3a-2127-422b-91ae-364da2661108	seclists.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

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

© 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](#) 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)

