CVE-2025-43400

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-43400
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-29 18:15:31 UTC
Updated	2026-04-02 19:20:39 UTC
Description	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 18.7.1 and iPadOS

Risk And Classification

Primary CVSS: v3.1 6.3 MEDIUM from ADP

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

Problem Types: CWE-787 | Processing a maliciously crafted font may lead to unexpected app termination or corrupt process memory | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
Low

Integrity
Low

Availability

Low

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

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	Ipados	26.0	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	26.0	All	All	All
Operating System	Apple	Macos	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apple	IOS And IPadOS	affected 18.7.1 custom	Not specified
CNA	Apple	IOS And IPadOS	affected 26.0.1 custom	Not specified
CNA	Apple	MacOS	affected 14.8.1 custom	Not specified
CNA	Apple	MacOS	affected 15.7.1 custom	Not specified
CNA	Apple	MacOS	affected 26.0.1 custom	Not specified
CNA	Apple	TvOS	affected 26.1 custom	Not specified
CNA	Apple	VisionOS	affected 26.0.1 custom	Not specified
CNA	Apple	WatchOS	affected 26.1 custom	Not specified

References

Reference	Source	Link	Tags
support.apple.com/en-us/125639	product-security@apple.com	support.apple.com	
seclists.org/fulldisclosure/2025/Sep/78	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
support.apple.com/en-us/125329	product-security@apple.com	support.apple.com	
support.apple.com/en-us/125330	product-security@apple.com	support.apple.com	
support.apple.com/en-us/125326	product-security@apple.com	support.apple.com	
support.apple.com/en-us/125327	product-security@apple.com	support.apple.com	
support.apple.com/en-us/125328	product-security@apple.com	support.apple.com	
seclists.org/fulldisclosure/2025/Sep/76	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
support.apple.com/en-us/125637	product-security@apple.com	support.apple.com	
support.apple.com/en-us/125338	product-security@apple.com	support.apple.com	
seclists.org/fulldisclosure/2025/Sep/73	af854a3a-2127-422b-91ae-364da2661108	seclists.org	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**