



# CVE-2025-43400

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

## Summary

<b>CVE</b>	CVE-2025-43400
<b>State</b>	PUBLISHED
<b>Assigner</b>	apple
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-29 18:15:31 UTC
<b>Updated</b>	2026-04-02 19:20:39 UTC
<b>Description</b>	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	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L</b>
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.3	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L</b>

## 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	<a href="#">Apple</a>	<a href="#">Ipados</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Ipados</a>	26.0	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	26.0	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Apple</a>	<a href="#">IOS And IPadOS</a>	affected 18.7.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">IOS And IPadOS</a>	affected 26.0.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 14.8.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 15.7.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 26.0.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">TvOS</a>	affected 26.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">VisionOS</a>	affected 26.0.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">WatchOS</a>	affected 26.1 custom	Not specified

### References

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

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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)