



# CVE-2025-43413

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

## Summary

<b>CVE</b>	CVE-2025-43413
<b>State</b>	PUBLISHED
<b>Assigner</b>	apple
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-11-04 02:15:47 UTC
<b>Updated</b>	2026-04-02 19:20:42 UTC
<b>Description</b>	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 26.1 and iPadOS 26.1, macOS

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from ADP

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

**Problem Types:** CWE-284 | CWE-693 | A sandboxed app may be able to observe system-wide network connections | CWE-693 CWE-693 Protection Mechanism Failure | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

#### 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="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	All	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Safari</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 26.1 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 14.8.2 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 15.7.2 custom	Not specified
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 26.1 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 26.1 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/125634">support.apple.com/en-us/125634</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/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>	Release Notes, Vendor Advisory
<a href="https://support.apple.com/en-us/125636">support.apple.com/en-us/125636</a>	<a href="mailto:product-security@apple.com">product-security@apple.com</a>	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
<a href="https://support.apple.com/en-us/125632">support.apple.com/en-us/125632</a>	<a href="mailto:product-security@apple.com">product-security@apple.com</a>	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
<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>	Vendor Advisory
<a href="https://support.apple.com/en-us/125638">support.apple.com/en-us/125638</a>	<a href="mailto:product-security@apple.com">product-security@apple.com</a>	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
<a href="https://support.apple.com/en-us/125635">support.apple.com/en-us/125635</a>	<a href="mailto:product-security@apple.com">product-security@apple.com</a>	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
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](#) 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](#).

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