



CVE-2025-24200

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

Summary

CVE	CVE-2025-24200
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-10 19:15:40 UTC
Updated	2026-04-03 11:44:27 UTC
Description	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.8.4 and iPadOS 15.8

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

EPSS: 0.478750000 probability, percentile 0.977020000 (date 2026-04-04)

CISA KEV: Listed on 2025-02-12; due 2025-03-05; ransomware use Unknown

Problem Types: CWE-863 | A physical attack may disable USB Restricted Mode on a locked device. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals. | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	ADP	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.1	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

None
Scope
Unchanged
Confidentiality
High
Integrity
High
Availability
None

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

CISA Known Exploited Vulnerability

Vendor	Apple
Product	iOS and iPadOS
Name	Apple iOS and iPadOS Incorrect Authorization 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/122173 ; https://nvd.nist.gov/vuln/detail/CVE-2025-24200

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 15.8.4 custom	Not specified
CNA	Apple	IOS And IPadOS	affected 16.7.11 custom	Not specified
CNA	Apple	IOS And IPadOS	affected 18.3.1 custom	Not specified
CNA	Apple	IPadOS	affected 17.7.5 custom	Not specified

References

Reference	Source	Link	Tags
seclists.org/fulldisclosure/2025/Feb/8	af854a3a-2127-422b-91ae-364da2661108	seclists.org	Mailing List, Third F
support.apple.com/en-us/122173	product-security@apple.com	support.apple.com	Release Notes, Ver
seclists.org/fulldisclosure/2025/Feb/7	af854a3a-2127-422b-91ae-364da2661108	seclists.org	Mailing List, Third F
seclists.org/fulldisclosure/2025/Apr/7	af854a3a-2127-422b-91ae-364da2661108	seclists.org	Mailing List, Third F
support.apple.com/en-us/122346	product-security@apple.com	support.apple.com	Release Notes, Ver
support.apple.com/en-us/122345	product-security@apple.com	support.apple.com	Release Notes, Ver
support.apple.com/en-us/122174	product-security@apple.com	support.apple.com	Release Notes, Ver

www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Government Re
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2025-02-12T00:00:00.000Z	CVE-2025-24200 added to CISA KEV

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