CVE-2025-24201

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-24201
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-11 18:15:30 UTC
Updated	2026-04-02 19:19:17 UTC
Description	An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in Sa

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: 0.000980000 probability, percentile 0.271250000 (date 2026-04-02)

CISA KEV: Listed on 2025-03-13; due 2025-04-03; ransomware use Unknown

Problem Types: CWE-787 | Maliciously crafted web content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.) | CWE-787 CWE-787 Out-of-bounds Write

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 WebKit Out-of-Bounds Write Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://support.apple.com/en-us/122281 ; https://support.apple.com/en-us/122283 ; https://support.apple.com/en-us/122284 ; https://support.apple.com/en-us/122285 ; ; https://nvd.nist.gov/vuln/detail/CVE-2025-24201

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	Macos	All	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Apple	Visionos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apple	Safari	affected 18.3.1 custom	Not specified
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 18.3.2 custom	Not specified
CNA	Apple	IPadOS	affected 17.7.6 custom	Not specified
CNA	Apple	MacOS	affected 15.3.2 custom	Not specified
CNA	Apple	VisionOS	affected 2.3.2 custom	Not specified

CNA	Apple	WatchOS	affected 11.4 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/122285	product-security@apple.com	support.apple.com
seclists.org/fulldisclosure/2025/Mar/4	af854a3a-2127-422b-91ae-364da2661108	seclists.org
lists.debian.org/debian-lts-announce/2025/06/msg00016.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
seclists.org/fulldisclosure/2025/Mar/5	af854a3a-2127-422b-91ae-364da2661108	seclists.org
github.com/cisagov/vulnrichment/issues/194	af854a3a-2127-422b-91ae-364da2661108	github.com
support.apple.com/en-us/122281	product-security@apple.com	support.apple.com
seclists.org/fulldisclosure/2025/Apr/7	af854a3a-2127-422b-91ae-364da2661108	seclists.org
support.apple.com/en-us/122346	product-security@apple.com	support.apple.com
support.apple.com/en-us/122283	product-security@apple.com	support.apple.com
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
support.apple.com/en-us/122345	product-security@apple.com	support.apple.com
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/Apr/16	af854a3a-2127-422b-91ae-364da2661108	seclists.org
seclists.org/fulldisclosure/2025/Mar/3	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/Mar/2	af854a3a-2127-422b-91ae-364da2661108	seclists.org
support.apple.com/en-us/122284	product-security@apple.com	support.apple.com
support.apple.com/en-us/122376	product-security@apple.com	support.apple.com
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 and Source URL Uptime Status status.cve.report