CVE-2025-43300

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-43300
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-21 01:15:36 UTC
Updated	2026-04-02 19:20:22 UTC
Description	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.8.5 and iPadOS

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from ADP

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

EPSS: 0.005480000 probability, percentile 0.678630000 (date 2026-04-02)

CISA KEV: Listed on 2025-08-21; due 2025-09-11; ransomware use Unknown

Problem Types: CWE-787 | Processing a malicious image file may result in memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals. | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
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	iOS, iPadOS, and macOS
Name	Apple iOS, iPadOS, and macOS 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/124925 ; https://support.apple.com/en-us/124926 ; https://support.apple.com/en-us/124927 ; https://support.apple.com/en-us/124928 ; https://support.apple.com/en-us/124929 ; https://nvd.nist.gov/vuln/detail/CVE-2025-43300

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 15.8.5 custom	Not specified
CNA	Apple	IOS And IPadOS	affected 16.7.12 custom	Not specified
CNA	Apple	IOS And IPadOS	affected 18.6.2 custom	Not specified
CNA	Apple	IPadOS	affected 17.7.10 custom	Not specified
CNA	Apple	MacOS	affected 13.7.8 custom	Not specified
CNA	Apple	MacOS	affected 14.7.8 custom	Not specified
CNA	Apple	MacOS	affected 15.6.1 custom	Not specified

References

Reference	Source	Link	Tags
support.apple.com/en-us/124927	product-security@apple.com	support.apple.com	
support.apple.com/en-us/124928	product-security@apple.com	support.apple.com	
support.apple.com/en-us/124925	product-security@apple.com	support.apple.com	

seclists.org/fulldisclosure/2025/Sep/52	af854a3a-2127-422b-91ae-364da2661108	seclists.org	Mailing Lis
support.apple.com/en-us/125141	product-security@apple.com	support.apple.com	Release N
support.apple.com/en-us/125142	product-security@apple.com	support.apple.com	Release N
github.com/cisagov/vulnrichment/issues/201	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Issue Trac
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Gover
github.com/b1n4r1b01/n-days/blob/main/CVE-2025-43300.md	af854a3a-2127-422b-91ae-364da2661108	github.com	Exploit, Th
support.apple.com/en-us/124929	product-security@apple.com	support.apple.com	
seclists.org/fulldisclosure/2025/Sep/10	af854a3a-2127-422b-91ae-364da2661108	seclists.org	Mailing Lis
support.apple.com/en-us/124926	product-security@apple.com	support.apple.com	
seclists.org/fulldisclosure/2025/Sep/14	af854a3a-2127-422b-91ae-364da2661108	seclists.org	Mailing Lis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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