



Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability

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

Summary

CVE	CVE-2023-41064
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-07 18:15:00 UTC
Updated	2023-09-22 00:15:00 UTC
Description	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 16.6.1 and iPadOS 16.6.1.

Risk And Classification

EPSS: 0.853530000 probability, percentile 0.993640000 (date 2026-04-14)

CISA KEV: Listed on 2023-09-11; due 2023-10-02; ransomware use Unknown

Problem Types: CWE-120

CISA Known Exploited Vulnerability

Vendor	Apple
Product	iOS, iPadOS, and macOS
Name	Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow 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/HT213905 , https://support.apple.com/en-us/HT213906 ; https://nvd.nist.gov/vuln/detail/CVE-2023-41064

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	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All

References

Reference	Source	Link	Tags
About the security content of macOS Monterey 12.0.0	MISC	support.apple.com	

About the security content of macOS Monterey 12.6.9 - Apple Support	MISC	support.apple.com	
About the security content of iOS 16.6.1 and iPadOS 16.6.1 - Apple Support	MISC	support.apple.com	
About the security content of macOS Ventura 13.5.2 - Apple Support	MISC	support.apple.com	
Full Disclosure: APPLE-SA-2023-09-11-3 macOS Big Sur 11.7.10	MISC	seclists.org	
Full Disclosure: APPLE-SA-2023-09-07-2 iOS 16.6.1 and iPadOS 16.6.1	MISC	seclists.org	
About the security content of iOS 15.7.9 and iPadOS 15.7.9 - Apple Support	MISC	support.apple.com	
About the security content of iOS 16.6.1 and iPadOS 16.6.1 - Apple Support	MISC	support.apple.com	
Full Disclosure: APPLE-SA-2023-09-11-2 macOS Monterey 12.6.9	MISC	seclists.org	
About the security content of macOS Ventura 13.5.2 - Apple Support	MISC	support.apple.com	
Full Disclosure: APPLE-SA-2023-09-11-1 iOS 15.7.9 and iPadOS 15.7.9	MISC	seclists.org	
Full Disclosure: APPLE-SA-2023-09-07-1 macOS Ventura 13.5.2	MISC	seclists.org	
About the security content of macOS Big Sur 11.7.10 - Apple Support	MISC	support.apple.com	
oss-security - CVE-2023-4863: libwebp: Heap buffer overflow in WebP Codec	MISC	www.openwall.com	
About the security content of macOS Big Sur 11.7.10 - Apple Support	MISC	support.apple.com	
About the security content of macOS Monterey 12.6.9 - Apple Support	MISC	support.apple.com	
About the security content of iOS 15.7.9 and iPadOS 15.7.9 - Apple Support	MISC	support.apple.com	
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.

Legacy QID Mappings

610526 Apple iOS 15.7.9 and iPadOS 15.7.9 Security Update Missing (HT213913)

© [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](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report