



CVE-2022-26764

Published on: Not Yet Published

Last Modified on: 06/08/2022 12:55:00 PM UTC

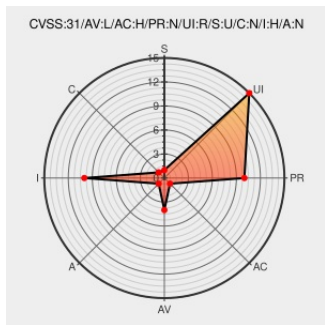
CVE-2022-26764

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **lpados** from **Apple** contain the following vulnerability:

A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.6, tvOS 15.5, macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.

CVE-2022-26764 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apple** - watchOS version < 8.6

Affected Vendor/Software: **Apple** - watchOS version < 15.5

Affected Vendor/Software: **Apple** - watchOS version < 12.4

Affected Vendor/Software: **Apple** - watchOS version < 15.5

CVSS3 Score: **4.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **2.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
About the security content of tvOS 15.5 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT213254
About the security content of watchOS 8.6 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT213253
About the security content of iOS 15.5 and iPadOS 15.5 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT213258
About the security content of macOS Monterey 12.4 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT213257

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [376612](#) Apple macOS Monterey 12.4 Not Installed (HT213257)
- [610416](#) Apple iOS 15.5 and iPadOS 15.5 Security Update Missing (HT213258)

Known Affected Configurations (CPE V2.3)

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
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

`cpe:2.3:o:apple:ipados:*:*:*:*:*:*:`

`cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:`






`cpe:2.3:o:apple:macos:*:*:*:*:*:*:`

`cpe:2.3:o:apple:tvos:*:*:*:*:*:*:`

`cpe:2.3:o:apple:watchos:*:*:*:*:*:*:`

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @iD7me	الهكر الشهير Linus 15.5 للاصدار الأمني في التقرير الصادر 15.4.1 ومادون في CVE-2022-26764 CV... twitter.com/i/web/status/1...	2022-05-18 01:02:18
 @CVEreport	CVE-2022-26764 : A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8... twitter.com/i/web/status/1...	2022-05-26 20:13:45
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-17 13:11:14
 /r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-18 14:59:44
 /r/netcve	CVE-2022-26764	2022-05-26 21:39:01

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2022   |

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