



CVE-2022-46720

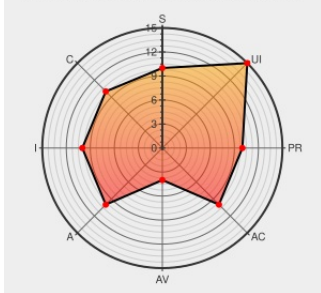
Published on: Not Yet Published

Last Modified on: 11/07/2023 03:55:00 AM UTC

CVE-2022-46720

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H



Certain versions of [Ipados](#) from [Apple](#) contain the following vulnerability:

An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2. An app may be able to break out of its sandbox

CVE-2022-46720 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apple** - macOS version < 13.1

Affected Vendor/Software: **Apple** - macOS version < 16.2

CVSS3 Score: **8.6 - HIGH**

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

CVE References

Description	Tags	Link
About the security content of macOS Ventura 13.1 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213532
About the security content of iOS 16.2 and iPadOS 16.2 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213530

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.

