



CVE-2022-26703

Published on: Not Yet Published

Last Modified on: 06/03/2022 01:52:00 PM UTC

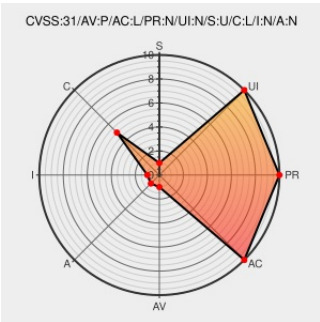
CVE-2022-26703

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.5 and iPadOS 15.5. A person with physical access to an iOS device may be able to access photos from the lock screen.

CVE-2022-26703 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: **Apple** - **iOS and iPadOS** version < 15.5

CVSS3 Score: **2.4 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
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

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






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
<code>cpe:2.3:o:apple:ipados:*:*:*:*:*:</code>						
<code>cpe:2.3:o:apple:iphone_os:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @management_sun	IT Risk: Apple.iOS 15.5,iPadOS 15.5のリリース情報が公開されました -5/5 CVE-2022-26731 CVE-2022-26766 CVE-2022-26703 CVE-2022-26700... twitter.com/i/web/status/1...	2022-05-16 23:29:42
 @manabu2111	Safariのプライベートブラウズモードで悪意のあるWebサイトに追跡される可能性がある「CVE-2022-26731」、デバイスを手に取れる人がロック画面から写真にアクセスできる可能性がある「CVE-2022-26703」もなど合わせて改善	2022-05-19 10:59:22
 /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-2022-26703	2022-05-26 20:38:24

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)