

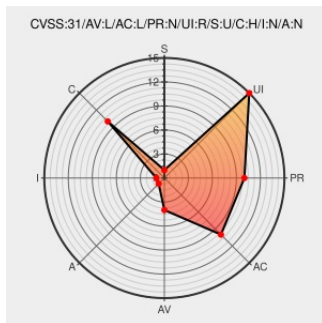


CVE-2021-1791

Published on: 04/02/2021 12:00:00 AM UTC

Last Modified on: 04/09/2021 10:17:00 PM UTC

CVE-2021-1791

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

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

An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose

kernel memory.

CVE-2021-1791 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apple** - iOS and iPadOS version < 14.4

Affected Vendor/Software: **Apple** - macOS version < 11.2

Affected Vendor/Software: **Apple** - macOS version < 7.3

Affected Vendor/Software: **Apple** - macOS version < 14.4

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **7.1 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

NONE

NONE

CVE References

Description	Tags	Link
About the security content of tvOS 14.4 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT212149
About the security content of macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT212147
About the security content of iOS 14.4 and iPadOS 14.4 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT212146
About the security content of watchOS 7.3 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT212148

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.

There are currently no QIDs associated with this CVE

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	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.14.6	-	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-004	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-005	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-006	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-007	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-001	All	All

Operating System	Apple	Mac Os X	10.14.6	security_update_2020-002	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-003	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-004	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-005	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-006	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-007	All	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update	All	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update_2	All	All
Operating System	Apple	Mac Os X	10.15.7	-	All	All
Operating System	Apple	Mac Os X	10.15.7	supplemental_update	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:mac_os_x:*:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:-:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2019-004:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2019-005:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2019-006:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2019-007:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2020-001:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2020-002:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2020-003:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2020-004:*:*:*:*:*:						
cpe:2.3:o:apple:mac os x:10.14.6:security update 2020-005:*:*:*:*:*:						

cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2020-006:*****:
cpe:2.3:o:apple:mac_os_x:10.14.6:security_update_2020-007:*****:
cpe:2.3:o:apple:mac_os_x:10.14.6:supplemental_update:*****:
cpe:2.3:o:apple:mac_os_x:10.14.6:supplemental_update_2:*****:
cpe:2.3:o:apple:mac_os_x:10.15.7:-:*****:
cpe:2.3:o:apple:mac_os_x:10.15.7:supplemental_update:*****:
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)
 @CVEreport	CVE-2021-1791 : An out-of-bounds read issue existed that led to the disclosure of #kernel memory. This was addresse... twitter.com/i/web/status/1...	2021-04-02 18:38:31

[← 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](#)