

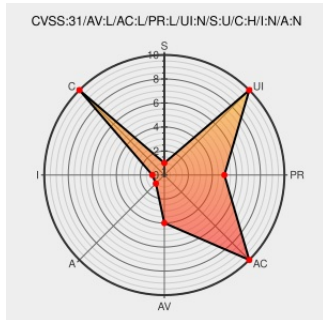


CVE-2020-9934

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 01/09/2023 04:41:00 PM UTC

CVE-2020-9934

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

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

An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A local user may be able to view sensitive user information.

CVE-2020-9934 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apple** - iOS version < iOS 13.6 and iPadOS 13.6

Affected Vendor/Software: **Apple** - macOS version < macOS Catalina 10.15.6

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	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
Apple iOS 13.6, iPadOS 13.6, macOS Catalina 10.15.6 CVE-2020-9934	CVE	CVE-2020-9934

About the security content of macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra - Apple Support

[Release Notes](#)
[Vendor Advisory](#)
[support.apple.com](#)
[text/html](#)

 [MISC](#)
[support.apple.com/HT211289](#)

About the security content of iOS 13.6 and iPadOS 13.6 - Apple Support

[Release Notes](#)
[Vendor Advisory](#)
[support.apple.com](#)
[text/html](#)

 [MISC](#)
[support.apple.com/HT211288](#)

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

Exploit/POC from Github

CVE-2020-9934 POC

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All

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

cpe:2.3:o:apple:ipad_os:*:*:*:*:*:

cpe:2.3:o:apple:ipad_os:*:*:*:*:*:

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

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

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @mattshockl	Seeing all of these great blog posts make me regret not giving CVE-2020-9934 a cool name! Maybe \$HOMERun? twitter.com/yo_yo_yo_jbo/s...	2022-01-10 18:47:27
 @patrickwardle	Neat TCC bypass & writeup by JBO ?? ...possible, as Apple's patch for CVE-2020-9934 was (as is often the case), inc... twitter.com/i/web/status/1...	2022-01-10 18:55:34
 @ESETresearch	On vulnerably Macs, CloudMensis exploits a known vulnerability known as CVE-2020-9934, to bypass TCC and gain acces... twitter.com/i/web/status/1...	2022-07-19 09:43:20
 @avoidthehack	Added includes: CVE-2022-3075 CVE-2022-28958 CVE-2022-27593 CVE-2022-26258 CVE-2020-9934 CVE-2018-7445 CVE-2018-6... twitter.com/i/web/status/1...	2022-09-08 20:25:11

[← 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](#)