

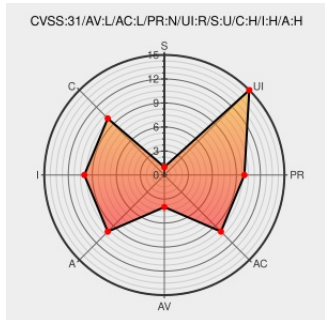


CVE-2020-9897

Published on: 10/28/2021 12:00:00 AM UTC

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

CVE-2020-9897

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

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

An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Big Sur 11.0.1. Processing a maliciously crafted PDF may lead to arbitrary code execution.

CVE-2020-9897 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apple** - **iOS and iPadOS** version < 14.2

Affected Vendor/Software: **Apple** - **macOS** version < 11.0

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Apple: CVE-2020-9897: iOS 14.2, iPadOS 14.2, macOS 11.0.1		Apple Security Update

About the security content of iOS 14.2 and iPadOS 14.2 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT211929
--	--	---

About the security content of macOS Big Sur 11.0.1 - Apple Support	support.apple.com text/html	 MISC support.apple.com/en-us/HT211931
--	--	---

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	Ipad Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
cpe:2.3:o:apple:ipados:*:*:*:*:*:						
cpe:2.3:o:apple:ipad_os:*:*:*:*:*:						
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:						
cpe:2.3:o:apple:macos:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ZecOps	Two new CVEs today for @ZecOps in @Apple's updates CVE-2021-30902 in Voice Control and CVE-2020-9897 in CoreGraphic... twitter.com/i/web/status/1...	2021-10-26 21:12:29
 @ZecOps	In the meantime, want to read more about CVE-2020-9897? Check this: blog.zecops.com/research/the-r...	2021-10-26 21:13:46
 @ipssignatures	The vuln CVE-2020-9897 has a tweet created 0 days ago and retweeted 11 times. twitter.com/ZecOps/status/... #pow1rtrtwwcve	2021-10-27 04:06:00
 @ipssignatures	The vuln CVE-2020-9897 has a tweet created 0 days ago and retweeted 10 times. twitter.com/ZecOps/status/... #pow1rtrtwwcve	2021-10-27 04:06:01
 @CVEreport	CVE-2020-9897 : An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.... twitter.com/i/web/status/1...	2021-10-28 19:05:52
 @WesUncensored	New vulnerability on the NVD: CVE-2020-9897 ift.tt/2XUQyG9	2021-10-28 20:33:32

 @workentin	New vulnerability on the NVD: CVE-2020-9897 ift.tt/2XUQyG9	2021-10-28 20:40:15
 @xanadulinux	CVE-2020-9897 ift.tt/2XUQyG9	2021-10-28 20:52:54

[< 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