



CVE-2020-9907

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

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

CVE-2020-9907

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to execute arbitrary code with kernel privileges.

CVE-2020-9907 has been assigned by [Apple](#) product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Apple](#) - iOS version < iOS 13.6 and iPadOS 13.6

Affected Vendor/Software: [Apple](#) - tvOS version < tvOS 13.4.8

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: **9.3 - HIGH**

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

CVE References

Description	Tags	Link
Apple - iOS 13.6 and iPadOS 13.6 - Memory Corruption Vulnerability	Apple, iOS, iPadOS, Memory Corruption, CVE-2020-9907	Apple Security Advisory - CVE-2020-9907

About the security content of tvOS 13.4.8 - Apple Support

Vendor Advisory

support.apple.com

text/html

 [MISC support.apple.com/H121290](https://support.apple.com/H121290)

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

Vendor Advisory

support.apple.com

text/html

 [MISC support.apple.com/HT211288](https://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

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	Tvos	All	All	All	All
Operating System	Apple	Tvos	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:tvos:*.***.***.***:						
cpe:2.3:o:apple:tvos:*.***.***.***:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)

 @42Sz40	@tim_cook @AppleSupport #applesupport CVE-2019-8795. CVE-2020-9907	2021-10-28 03:53:16
 @inthewildio	Also here is a list: CVE-2018-4344 CVE-2019-8605 CVE-2020-3837 CVE-2020-9907 CVE-2021-4034 CVE-2022-29499 CVE-2016... twitter.com/i/web/status/1...	2022-08-07 20:16:07
 @ZecOps	From #OBTS conference today: Ian Beer from @projectzero mentioned that CVE-2020-9907 was exploited in the wild. Tha... twitter.com/i/web/status/1...	2022-10-06 19:38:49
 @ipssignatures	The vuln CVE-2020-9907 has a tweet created 0 days ago and retweeted 10 times. twitter.com/ZecOps/status/... #pow1rtrtwwcve	2022-10-07 04:06:00
 /r/SecurityIT	Spyware made in Italy	2022-06-18 00:21:56
← 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](#)