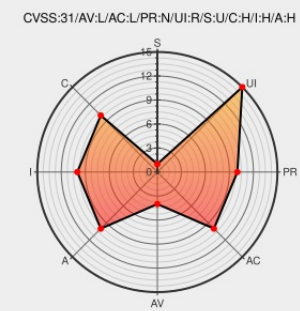
CVE-2021-1816

Published on: 09/08/2021 12:00:00 AM UTC

Last Modified on: 09/20/2021 08:08:00 PM UTC

CVE-2021-1816

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ipados from Apple contain the following vulnerability:

A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. A malicious application may be able to execute arbitrary code with kernel privileges.

CVE-2021-1816 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 **< 14.5**

Affected Vendor/Software: **Apple** - **tvOS** version **< 14.5**

Affected Vendor/Software: **Apple** - **watchOS** version **< 7.4**

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
About the security content of watchOS 7.4 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT212324
About the security content of tvOS 14.5 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT212323
About the security content of iOS 14.5 and iPadOS 14.5 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT212317

Related QID Numbers

610334 Apple iOS 14.5 and iPadOS 14.5 Security Update Missing (HT212317)

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	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:tvos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@HuseyinKabasa	@WangTielei Are you planning to do a write up about CVE-2021-1816 ?	2021-06-10 10:16:50
@b1n4r1b01	@WangTielei Hi, is the ApplePPM bug from your MOSEC talk CVE-2021-1816? Can't trigger the posted POC on my device for some reason?	2021-08-04 11:00:52

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report