

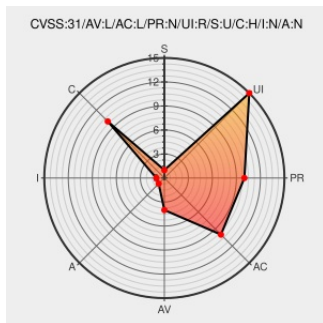


CVE-2019-8540

Published on: 12/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:56 PM UTC

CVE-2019-8540

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

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

A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout.

CVE-2019-8540 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apple** - **iOS** version < **iOS 12.2**

Affected Vendor/Software: **Apple** - **macOS** version < **macOS Mojave 10.14.4**

Affected Vendor/Software: **Apple** - **tvOS** version < **tvOS 12.2**

Affected Vendor/Software: **Apple** - **watchOS** version < **watchOS 5.2**

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 12.2 - Apple Support	Vendor Advisory support.apple.com text/html	 MISC support.apple.com/HT209601
About the security content of iOS 12.2 - Apple Support	Vendor Advisory support.apple.com text/html	 MISC support.apple.com/HT209599
About the security content of watchOS 5.2 - Apple Support	Vendor Advisory support.apple.com text/html	 MISC support.apple.com/HT209602
About the security content of macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra - Apple Support	Vendor Advisory support.apple.com text/html	 MISC support.apple.com/HT209600

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

Kernel Stack info leak at exportObjectToClient function

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

```
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:*****:
cpe:2.3:o:apple:tvos:*****:
cpe:2.3:o:apple:tvos:*****:
cpe:2.3:o:apple:watchos:*****:
cpe:2.3:o:apple:watchos:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)