

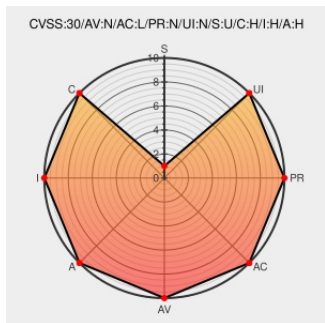


CVE-2018-4331

Published on: 04/03/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:15 PM UTC

CVE-2018-4331

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

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

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12, macOS Mojave 10.14, tvOS 12, watchOS 5.

CVE-2018-4331 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

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

CVE References

Description	Tags	Link
About the security content of macOS Mojave 10.14 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/kb/HT209139
About the security content of watchOS 5 - Apple Support	Vendor Advisory	MISC

support.apple.com/kb/HT209108

Vendor Advisory
support.apple.com
text/html

 MISC

Vendor Advisory
support.apple.com
text/html

 MISC

Vendor Advisory
support.apple.com
text/html

 MISC

comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2018-4331: Exploit for a race condition in the GSSCred system service on iOS 11.2.

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 →](#)

© 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