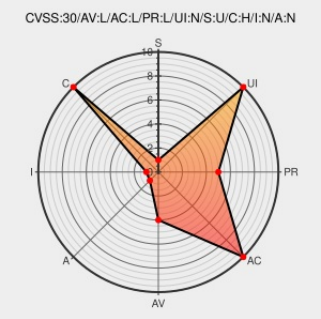
CVE-2018-4431

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

Last Modified on: 03/23/2021 11:24:16 PM UTC

CVE-2018-4431

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 affected versions prior to iOS 12.1.1, macOS Mojave 10.14.2, tvOS 12.1.1, watchOS 5.1.2.

CVE-2018-4431 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	NONE

CVE References

Description	Tags	Link
About the security content of watchOS 5.1.2 - Apple Support	Vendor Advisory, support.apple.com, text/html	MISC support.apple.com/kb/HT209343
About the security content of iOS 12.1.1 - Apple Support	Vendor Advisory	MISC

	support.apple.com text/html	support.apple.com/kb/HT209340
About the security content of tvOS 12.1.1 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/kb/HT209342
About the security content of macOS Mojave 10.14.2, Security Update 2018-003 High Sierra, Security Update 2018-006 Sierra - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/kb/HT209341

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC Exploit iOS 12 to iOS 12.1 (CVE-2018-4431)

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→