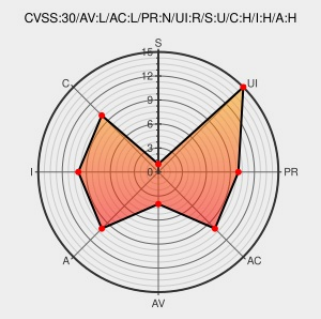
CVE-2018-4150

Published on: 04/03/2018 12:00:00 AM UTC

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

CVE-2018-4150

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



Certain versions of Iphone Os from Apple contain the following vulnerability:

An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.

CVE-2018-4150 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

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 macOS/OS X Multiple Flaws Let Remote Users Bypass Security and Obtain Potentially Sensitive Information and Let Local Users Obtain Passwords	Third Party Advisory VDB Entry	SECTRACK 1040608

and Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	
About the security content of iOS 11.3 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT208693
About the security content of macOS High Sierra 10.13.4, Security Update 2018-002 Sierra, and Security Update 2018-002 El Capitan - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT208692
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Spoof the User Interface, Remote and Local Users Bypass Security Restrictions and Obtain Potentially Sensitive Information, and Let Applications Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1040604
About the security content of watchOS 4.3 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT208696
About the security content of tvOS 11.3 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT208698

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Proof of concept for CVE-2018-4150 by @cmwdotme

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 and Source URL Uptime Status status.cve.report