



CVE-2016-1807

Published on: 05/20/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

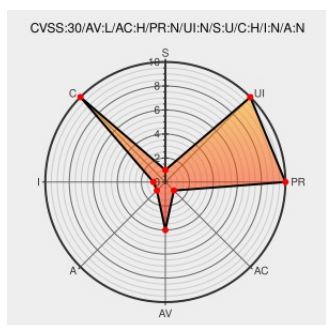
CVE-2016-1807

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Race condition in the Disk Images subsystem in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows local users to obtain sensitive information from kernel memory via unspecified vectors.

CVE-2016-1807 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.1 - MEDIUM**

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

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
About the security content of OS X El Capitan v10.11.5 and Security Update 2016-003 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT206567
APPLE-SA-2016-05-16-2 iOS 9.3.2	Mailing List	APPLE APPLE-SA-2016-05-16-2

	Vendor Advisory lists.apple.com text/html	
OS X / iOS Kernel IOHDXControllerUserClient Use-After-Free ~ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/137395/OS-X-iOS-Kernel-IOHDXControllerUserClient-Use-After-Free.html
732 - OS X/iOS kernel UAF racing getProperty on IOHDXController and testNetBootMethod on IOHDXControllerUserClient - project-zero - Monorail	Exploit Third Party Advisory bugs.chromium.org text/html	 MISC bugs.chromium.org/p/project-zero/issues/detail?id=732
APPLE-SA-2016-05-16-4 OS X El Capitan 10.11.5 and Security Update 2016-003	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-4
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Remote and Local Users Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1035890
Apple - Lists.apple.com	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-1
Apple Mac OSX / iOS Kernel - UAF Racing getProperty on IOHDXController and testNetBootMethod on IOHDXControllerUserClient - Multiple dos Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39929
About the security content of tvOS 9.2.1 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206564
APPLE-SA-2016-05-16-3 watchOS 2.2.1	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-3
About the security content of iOS 9.3.2 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206568
About the security content of watchOS 2.2.1 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206566
No Description Provided	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 90694

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

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→

