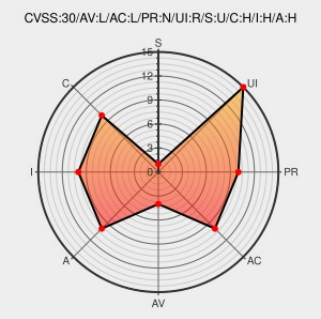
CVE-2016-1819

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

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

CVE-2016-1819

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



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

Use-after-free vulnerability in the IOAccelContext2::clientMemoryForType method 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 attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1817 and CVE-2016-1818.

CVE-2016-1819 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
772 - OS X kernel use-after-free due to bad locking in IOAcceleratorFamily2 - project-zero - Monorail	Exploit, Third Party Advisory	MISC bugs.chromium.org/p/project-zero/issues/detail?id=772

	bugs.chromium.org text/html	
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 Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-05-16-2
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
About the security content of tvOS 9.2.1 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT206564
Apple Mac OSX Kernel - Use-After-Free Due to Bad Locking in IOAcceleratorFamily2 - OSX dos Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39928
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
OS X Kernel Use-After-Free From IOAcceleratorFamily2 Bad Locking ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/137396/OS-X-Kernel-Use-After-Free-From-IOAcceleratorFamily2-Bad-Locking.html

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→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report