



CVE-2016-1719

Published on: 02/01/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:05 PM UTC

CVE-2016-1719

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

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

The IOHIDFamily API in Apple iOS before 9.2.1, OS X before 10.11.3, and tvOS before 9.1.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.

CVE-2016-1719 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	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
iOS Kernel AppleOscarGyro Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/135443/iOS-Kernel-AppleOscarGyro-Use-After-Free.html
iOS Kernel - AppleOscarAccelerometer Use-After-Free - iOS	www.exploit-db.com	EXPLOIT-DB 39360

dos Exploit	Proof of Concept text/html	
APPLE-SA-2016-03-21-2 watchOS 2.2	lists.apple.com text/html	 APPLE APPLE-SA-2016-03-21-2
About the security content of tvOS 9.1.1 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT205729
About the security content of iOS 9.2.1 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT205732
iOS Kernel AppleOscarAccelerometer Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135442/iOS-Kernel-AppleOscarAccelerometer-Use-After-Free.html
iOS Kernel - AppleOscarCMA Use-After-Free - iOS dos Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39362
iOS Kernel - AppleOscarGyro Use-After-Free - iOS dos Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39359
603 - project-zero - Project Zero - Monorail	code.google.com text/html	 MISC code.google.com/p/google-security-research/issues/detail?id=603
APPLE-SA-2016-01-19-1 iOS 9.2.1	Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-01-19-1
About the security content of OS X El Capitan 10.11.3 and Security Update 2016-001 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT205731
iOS Kernel - IOReportHub Use-After-Free - iOS dos Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39364
About the security content of watchOS 2.2 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206168
iOS Kernel AppleOscarCMA Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135440/iOS-Kernel-AppleOscarCMA-Use-After-Free.html
604 - project-zero - Project Zero - Monorail	code.google.com text/html	 MISC code.google.com/p/google-security-research/issues/detail?id=604
APPLE-SA-2016-01-19-2 OS X El Capitan 10.11.3 and Security Update 2016-001	Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-01-19-2
APPLE-SA-2016-01-25-1 tvOS 9.1.1	Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-01-25-1
606 - project-zero - Project Zero - Monorail	code.google.com text/html	 MISC code.google.com/p/google-security-research/issues/detail?id=606
608 - project-zero - Project Zero - Monorail	code.google.com text/html	 MISC code.google.com/p/google-security-research/issues/detail?id=608
iOS Kernel - AppleOscarCompass Use-After-Free - iOS dos Exploit	www.exploit-db.com Proof of Concept	 EXPLOIT-DB 39361

	text/html	
iOS Kernel AppleOscarCompass Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135441/iOS-Kernel-AppleOscarCompass-Use-After-Free.html
iOS Kernel IOReportHub Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135438/iOS-Kernel-IOReportHub-Use-After-Free.html
607 - project-zero - Project Zero - Monorail	code.google.com text/html	 MISC code.google.com/p/google-security-research/issues/detail?id=607
Apple OS X Multiple Memory Corruption Flaws Lets Local Users Obtain Root Privileges - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1034736
605 - project-zero - Project Zero - Monorail	code.google.com text/html	 MISC code.google.com/p/google-security-research/issues/detail?id=605
iOS Kernel IOHIDEventService Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135439/iOS-Kernel-IOHIDEventService-Use-After-Free.html
iOS Kernel - IOHIDEventService Use-After-Free - iOS dos Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39363

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	Mac Os X	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

```
cpe:2.3:o:apple:iphone_os:*.:.:.:.:.:.:.:
```

```
cpe:2.3:o:apple:mac os x:*.:.:.:.:.:.:
```

```
cpe:2.3:o:apple:tvos:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:apple:watchos:*.:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

© [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](#)