CVE-2016-1803

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-1803
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-20 10:59:00 UTC
Updated	2019-03-25 17:54:00 UTC
Description	CoreCapture 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 attacker

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
About the security content of OS X El Capitan v10.11.5 and Security Update 2016-003 - Apple Support
APPLE-SA-2016-05-16-2 iOS 9.3.2
APPLE-SA-2016-05-16-4 OS X El Capitan 10.11.5 and Security Update 2016-003
ZDI-16-339 | Zero Day Initiative
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Remote and Local Users Obtain Potentially Se
Apple - Lists.apple.com

777 - OS X exploitable kernel NULL dereference in CoreCaptureResponder due to unchecked return value - project-zero - Monorail
About the security content of tvOS 9.2.1 - Apple Support
APPLE-SA-2016-05-16-3 watchOS 2.2.1
About the security content of iOS 9.3.2 - Apple Support
About the security content of watchOS 2.2.1 - Apple Support
90694
Apple Mac OSX Kernel - NULL Dereference in CoreCaptureResponder Due to Unchecked Return Value - OSX dos Exploit
OS X CoreCaptureResponder NULL Pointer Dereference ≈ Packet Storm
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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