CVE-2017-13876

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

Summary

CVE	CVE-2017-13876
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-25 21:29:00 UTC
Updated	2019-03-08 16:06:00 UTC
Description	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS be

Risk And Classification

Problem Types: CWE-119

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 watchOS 4.2 - Apple Support
Apple TV Bugs Let Remote Users Execute Arbitrary Code and Let Local Users View Memory Contents and Gain Elevated Privileges - Securit
About the security content of iOS 11.2 - Apple Support
Apple macOS/OS X Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information and Let Local Users Deny Service, View Files,
Apple iOS/WatchOS/tvOS/macOS Multiple Security Vulnerabilities
About the security content of macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan - Apple

Apple iOS Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information and Let Local Users View Memory Co
Apple XNU Kernel - Memory Corruption due to Integer Overflow in __offsetof Usage in posix_spawn on 32-bit Platforms - Multiple dos Exploit
About the security content of tvOS 11.2 - Apple Support
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**