



CVE-2014-4461

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-4461
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-18 11:59:00 UTC
Updated	2019-03-08 16:06:00 UTC
Description	The kernel in Apple iOS before 8.1.1 and Apple TV before 7.0.2 does not properly validate IOSharedDataQueue object met

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	8.0	All	All	All
Operating System	Apple	Iphone Os	8.0.1	All	All	All
Operating System	Apple	Iphone Os	8.0.2	All	All	All
Operating System	Apple	Iphone Os	8.0	All	All	All
Operating System	Apple	Iphone Os	8.0.1	All	All	All
Operating System	Apple	Iphone Os	8.0.2	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	10.10.0	All	All	All
Operating System	Apple	Mac Os X	10.8.5	All	All	All
Operating System	Apple	Mac Os X	10.9.5	All	All	All
Operating System	Apple	Mac Os X	10.10.0	All	All	All
Operating System	Apple	Mac Os X	10.8.5	All	All	All
Operating System	Apple	Mac Os X	10.9.5	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Tv os	6.0	All	All	All
Operating System	Apple	Tv os	6.0.1	All	All	All
Operating System	Apple	Tv os	6.0.2	All	All	All

Operating System	Apple	Tvos	6.1	All	All	All
Operating System	Apple	Tvos	6.1.1	All	All	All
Operating System	Apple	Tvos	6.1.2	All	All	All
Operating System	Apple	Tvos	6.2	All	All	All
Operating System	Apple	Tvos	6.2.1	All	All	All
Operating System	Apple	Tvos	7.0	All	All	All
Operating System	Apple	Tvos	6.0	All	All	All
Operating System	Apple	Tvos	6.0.1	All	All	All
Operating System	Apple	Tvos	6.0.2	All	All	All
Operating System	Apple	Tvos	6.1	All	All	All
Operating System	Apple	Tvos	6.1.1	All	All	All
Operating System	Apple	Tvos	6.1.2	All	All	All
Operating System	Apple	Tvos	6.2	All	All	All
Operating System	Apple	Tvos	6.2.1	All	All	All
Operating System	Apple	Tvos	7.0	All	All	All
Operating System	Apple	Tvos	All	All	All	All

References						
Reference				Source	Link	
IBM X-Force Exchange				XF	excha	
About the security content of Apple TV 7.0.2 - Apple Support				CONFIRM	suppc	
Apple iOS and TV CVE-2014-4461 Remote Code Execution Vulnerability				BID	www.i	
About the security content of OS X Yosemite v10.10.2 and Security Update 2015-001 - Apple Support				CONFIRM	suppc	
About the security content of iOS 8.1.1 - Apple Support				CONFIRM	suppc	
APPLE-SA-2014-11-17-1 iOS 8.1.1				APPLE	lists.a	
Apple - Lists.apple.com				APPLE	lists.a	
About the security content of iOS 8.1.1 - Apple Support				CONFIRM	suppc	
Apple TV Bugs Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges - SecurityTracker				SECTrack	www.i	
APPLE-SA-2015-01-27-4 OS X 10.10.2 and Security Update 2015-001				APPLE	lists.a	
About the security content of Apple TV 7.0.2 - Apple Support				CONFIRM	suppc	
CVE Program record				CVE.ORG	www.i	
NVD vulnerability detail				NVD	nvd.n	

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)