



CVE-2015-5925

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

Summary

CVE	CVE-2015-5925
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-23 21:59:00 UTC
Updated	2016-12-24 02:59:00 UTC
Description	The CoreGraphics component in Apple iOS before 9.1, OS X before 10.11.1, and watchOS before 2.0.1 allows remote att

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

References

Reference
APPLE-SA-2015-10-21-4 OS X El Capitan 10.11.1 and Security Update 2015-007
APPLE-SA-2015-10-21-2 watchOS 2.0.1
About the security content of iOS 9.1 - Apple Support
About the security content of OS X El Capitan 10.11.1, Security Update 2015-004 Yosemite, and Security Update 2015-007 Mavericks - Apple
Apple OS X Multiple Flaws Let Remote Users Execute Arbitrary Code and Let Apps Gain Elevated Privileges - SecurityTracker
About the security content of watchOS 2.0.1 - Apple Support
APPLE-SA-2015-10-21-1 iOS 9.1
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.

© [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](#).

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