



CVE-2015-3800

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

Summary

CVE	CVE-2015-3800
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-17 00:00:00 UTC
Updated	2016-12-24 02:59:00 UTC
Description	The DiskImages component in Apple iOS before 8.4.1 and OS X before 10.10.5 allows local users to gain privileges or cause a denial of service (DoS) by exploiting a buffer overflow in the diskimages component.

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

References

Reference
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Deny Service and Let Apps
Apple Mac OS X and iOS Multiple Security Vulnerabilities
About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support
About the security content of iOS 8.4.1 - Apple Support
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006
APPLE-SA-2015-08-13-3 iOS 8.4.1
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](#).

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

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