



CVE-2015-5889

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

Summary

CVE	CVE-2015-5889
State	PUBLIC
Assigner	product-security@apple.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-09 05:59:00 UTC
Updated	2016-12-24 02:59:00 UTC
Description	rsh in the remote_cmds component in Apple OS X before 10.11 allows local users to obtain root privileges via vectors invol

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All

References

Reference
Mac OS X 10.9.5 / 10.10.5 rsh/libmalloc Privilege Escalation ~ Packet Storm
Apple OS X Multiple Flaws Let Remote and Local Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Deny Service a
APPLE-SA-2015-09-30-3 OS X El Capitan 10.11
CVE-2015-5889 Mac OS X 10.9.5 / 10.10.5 - rsh/libmalloc Privilege Escalation Rapid7
Apple Mac OS X Prior to 10.11 Multiple Security Vulnerabilities
Full Disclosure: Mac OS X local root (rsh/libmalloc)
issetugid() + rsh + libmalloc OS X Local Root ~ Packet Storm
Exploit – Page 38540 – Exploits Database
Mac OS X 10.9.5 / 10.10.5 - rsh/libmalloc Privilege Escalation
About the security content of OS X El Capitan v10.11 - 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.

© [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](#)