



CVE-2014-1419

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-1419
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-24 14:55:00 UTC
Updated	2017-01-07 02:59:00 UTC
Description	Race condition in the power policy functions in policy-funcs in acpi-support before 0.142 allows local users to gain privileges

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Acpi-support	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All

References

Reference	Source	Link
USN-2297-1: acpi-support vulnerability Ubuntu	UBUNTU	www.ubuntu.com
About Secunia Research Flexera	SECUNIA	secunia.com
Debian -- Security Information -- DSA-2984-1 acpi-support	DEBIAN	www.debian.org
Bug #1340812 "Privilege escalation vulnerability in power policy..." : Bugs : "acpi-support" package : Ubuntu	CONFIRM	bugs.launchpad.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)