



CVE-2014-0476

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

Summary

CVE	CVE-2014-0476
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-25 22:55:00 UTC
Updated	2017-09-19 01:36:00 UTC
Description	The slapper function in chkrootkit before 0.50 does not properly quote file paths, which allows local users to execute arbitra

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	All	Its	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	All	Its	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Application	Chkrootkit	Chkrootkit	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-2945-1 chkrootkit	DEBIAN	www.debian.org	
chkrootkit: Local privilege escalation (GLSA 201709-05) — Gentoo security	GENTOO	security.gentoo.org	
107710	OSVDB	osvdb.org	
Chkrootkit Local Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
Chkrootkit - Privilege Escalation (Metasploit)	EXPLOIT-DB	www.exploit-db.com	

chkrootkit -- locally checks for signs of a rootkit	CONFIRM	www.chkrootkit.org	Vendor Advisory
USN-2230-1: chkrootkit vulnerability Ubuntu	UBUNTU	www.ubuntu.com	
oss-security - CVE-2014-0476 chkrootkit vulnerability	MLIST	www.openwall.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710350](#) Gentoo Linux chkrootkit Local privilege escalation Vulnerability (GLSA 201709-05)

© [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