



CVE-2014-9680

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

Summary

CVE	CVE-2014-9680
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-24 06:59:00 UTC
Updated	2018-01-05 02:29:00 UTC
Description	sudo before 1.8.12 does not ensure that the TZ environment variable is associated with a zoneinfo file, which allows local u

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sudo Project	Sudo	All	p2	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Sudo TZ Environment Variable Flaw Lets Local Users Modify Data on the Target System - SecurityTracker	SECTRACK	www.securitytrac
sudo: Information disclosure (GLSA 201504-02) — Gentoo security	GENTOO	security.gentoo.o
oss-security - Abusing TZ for fun (and little profit)	MLIST	openwall.com
Arbitrary file access via TZ environment variable	CONFIRM	www.sudo.ws
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[390227](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for sudo (OVMSA-2021-0012)

© [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](#)