



# CVE-2021-23240

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-23240
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-12 09:15:00 UTC
<b>Updated</b>	2023-11-07 03:30:00 UTC
<b>Description</b>	selinux_edit_copy_tfiles in sudoedit in Sudo before 1.9.5 allows a local unprivileged user to gain file ownership and escalate

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Application	<a href="#">Sudo Project</a>	<a href="#">Sudo</a>	All	All	All	All
Application	<a href="#">Sudo Project</a>	<a href="#">Sudo</a>	All	All	All	All

## References

Reference
[SECURITY] Fedora 32 Update: sudo-1.9.5p1-1.fc32 - package-announce - Fedora Mailing-Lists
January 2021 Sudo Vulnerabilities in NetApp Products   NetApp Product Security
[bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgr
Pony Mail!

Bug 1180685 – VUL-0: CVE-2021-23240: sudo: Possible Symlink Attack in SELinux Context in `sudoedit`

Sudo Stable Release

[SECURITY] Fedora 33 Update: sudo-1.9.5p1-1.fc33 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 33 Update: sudo-1.9.5p1-1.fc33 - package-announce - Fedora Mailing-Lists

Pony Mail!

[bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade

sudo: Multiple vulnerabilities (GLSA 202101-33) — Gentoo security

[SECURITY] Fedora 32 Update: sudo-1.9.5p1-1.fc32 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159207](#) Oracle Enterprise Linux Security Update for sudo (ELSA-2021-1723)

[179654](#) Debian Security Update for sudo (CVE-2021-23240)

[239316](#) Red Hat Update for sudo (RHSA-2021:1723)

[377324](#) Alibaba Cloud Linux Security Update for sudo (ALINUX3-SA-2022:0113)

[500677](#) Alpine Linux Security Update for sudo

[670208](#) EulerOS Security Update for sudo (EulerOS-SA-2021-1707)

[900097](#) CBL-Mariner Linux Security Update for sudo 1.8.31p1

[902910](#) Common Base Linux Mariner (CBL-Mariner) Security Update for sudo (3728)

[940285](#) AlmaLinux Security Update for sudo (ALSA-2021:1723)

[960837](#) Rocky Linux Security Update for sudo (RLSA-2021:1723)

© [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](#)