



# CVE-2022-43995

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

## Summary

<b>CVE</b>	CVE-2022-43995
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-02 14:15:00 UTC
<b>Updated</b>	2022-12-06 00:15:00 UTC
<b>Description</b>	Sudo 1.8.0 through 1.9.12, with the crypt() password backend, contains a plugins/sudoers/auth/passwd.c array-out-of-boun

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sudo Project</a>	<a href="#">Sudo</a>	All	All	All	All
Application	<a href="#">Sudo Project</a>	<a href="#">Sudo</a>	1.9.12	-	All	All
Application	<a href="#">Sudo Project</a>	<a href="#">Sudo</a>	All	All	All	All

## References

Reference	Source	Link
Security Advisories   Sudo	MISC	<a href="#">www.sudo.</a>
sudo: Heap-Based Buffer Overread (GLSA 202211-08) — Gentoo security	GENTOO	<a href="#">security.ge</a>
2139911 – (CVE-2022-43995) CVE-2022-43995 sudo: heap-based overflow with very small passwords	MISC	<a href="#">bugzilla.rec</a>
Sudo: Heap-based overflow with small passwords   Hacker News	MISC	<a href="#">news.ycom</a>
Fix CVE-2022-43995, potential heap overflow for passwords < 8 charact... · sudo-project/sudo@bd209b9 · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.o</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.go</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">182565</a> Debian Security Update for sudo (CVE-2022-43995)
<a href="#">355189</a> Amazon Linux Security Advisory for sudo : ALAS2023-2023-106
<a href="#">502640</a> Alpine Linux Security Update for sudo
<a href="#">672490</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1047)
<a href="#">672507</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1022)
<a href="#">672551</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1137)
<a href="#">672553</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1113)
<a href="#">672608</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1337)
<a href="#">672623</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1400)
<a href="#">672646</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1372)
<a href="#">672764</a> EulerOS Security Update for sudo (EulerOS-SA-2023-1516)
<a href="#">690976</a> Free Berkeley Software Distribution (FreeBSD) Security Update for sudo (3310014a-5ef9-11ed-812b-206a8a720317)
<a href="#">710681</a> Gentoo Linux sudo Heap-Based Buffer Overread Vulnerability (GLSA 202211-08)
<a href="#">752784</a> SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2022:3938-1)
<a href="#">752805</a> SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2022:4001-1)
<a href="#">752856</a> SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2022:4240-1)
<a href="#">752928</a> SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2022:4077-1)
<a href="#">752942</a> SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2022:4280-1)
<a href="#">904438</a> Common Base Linux Mariner (CBL-Mariner) Security Update for sudo (11423)
<a href="#">904471</a> Common Base Linux Mariner (CBL-Mariner) Security Update for sudo (11400)
<a href="#">904534</a> Common Base Linux Mariner (CBL-Mariner) Security Update for sudo (11423-1)
<a href="#">904586</a> Common Base Linux Mariner (CBL-Mariner) Security Update for sudo (11400-1)

© [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](#)**