



# CVE-2022-2989

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

## Summary

<b>CVE</b>	CVE-2022-2989
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-13 14:15:00 UTC
<b>Updated</b>	2023-02-12 22:15:00 UTC
<b>Description</b>	An incorrect handling of the supplementary groups in the Podman container engine might lead to the sensitive information c

## Risk And Classification

**Problem Types:** CWE-842

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Podman Project</a>	<a href="#">Podman</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.11	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.0	All	All	All

## References

Reference	Source	Link
Vulnerability in Linux containers – investigation and mitigation – Bentham’s Gaze	MISC	<a href="http://www.benthamsgaze.com">www.benthamsgaze.com</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
2121445 – (CVE-2022-2989) CVE-2022-2989 podman: possible information disclosure and modification	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">160285</a> Oracle Enterprise Linux Security Update for buildah (ELSA-2022-8008)
<a href="#">160318</a> Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2022-7822)
<a href="#">160323</a> Oracle Enterprise Linux Security Update for podman (ELSA-2022-8431)
<a href="#">160696</a> Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2023-2802)
<a href="#">182066</a> Debian Security Update for libpod (CVE-2022-2989)
<a href="#">199663</a> Ubuntu Security Notification for Podman Vulnerability (USN-6295-1)
<a href="#">240848</a> Red Hat Update for container-tools:rhel8 security (RHSA-2022:7822)
<a href="#">240894</a> Red Hat Update for buildah (RHSA-2022:8008)
<a href="#">240912</a> Red Hat Update for podman security (RHSA-2022:8431)
<a href="#">241486</a> Red Hat Update for container-tools:4.0 (RHSA-2023:2802)
<a href="#">379641</a> Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050)
<a href="#">502914</a> Alpine Linux Security Update for podman
<a href="#">505793</a> Alpine Linux Security Update for podman
<a href="#">753196</a> SUSE Enterprise Linux Security Update for podman (SUSE-SU-2022:3819-1)
<a href="#">753482</a> SUSE Enterprise Linux Security Update for podman (SUSE-SU-2022:3820-1)
<a href="#">753592</a> SUSE Enterprise Linux Security Update for podman (SUSE-SU-2023:0187-1)
<a href="#">753659</a> SUSE Enterprise Linux Security Update for podman (SUSE-SU-2023:0326-1)
<a href="#">903958</a> Common Base Linux Mariner (CBL-Mariner) Security Update for podman (10964)
<a href="#">904613</a> Common Base Linux Mariner (CBL-Mariner) Security Update for podman (11521)
<a href="#">906919</a> Common Base Linux Mariner (CBL-Mariner) Security Update for podman (10964-1)
<a href="#">940780</a> AlmaLinux Security Update for container-tools:rhel8 (ALSA-2022:7822)
<a href="#">940785</a> AlmaLinux Security Update for podman (ALSA-2022:8431)
<a href="#">940827</a> AlmaLinux Security Update for buildah (ALSA-2022:8008)
<a href="#">941090</a> AlmaLinux Security Update for container-tools:4.0 (ALSA-2023:2802)
<a href="#">960180</a> Rocky Linux Security Update for container-tools:rhel8 (RLSA-2022:7822)

---

© [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](#)**