



# Bug 2317467 (CVE-2024-9676) - CVE-2024-9676 Podman: Buildah: CRI-O: symlink traversal vulnerability in the containers/storage library can cause Denial of Service (DoS)

**Keywords:** Security

**Reported:** 2024-10-09 03:04 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2025-04-11 10:53 UTC ([History](#))

**Alias:** CVE-2024-9676

**CC List:** 21 users ([show](#))

**Deadline:** 2024-10-15

**Fixed In Version:**

**Product:** Security Response

**Clone Of:**

**Component:** vulnerability

**Environment:**

**Version:** unspecified

**Last Closed:**

**Hardware:** All

**Embargoed:**

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [2319015](#) [2319016](#) [2319017](#)  
[2319018](#) [2319019](#) [2319020](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)


## Attachments [\(Terms of Use\)](#)

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHBA-2024:10810</a>	0	None	None	None	2024-12-04 21:22:04 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:10289</a>	0	None	None	None	2024-11-26 06:43:28 UTC

Red Hat Product Errata	<a href="#">RHSA-2024:8418</a>	0	None	None	None	2024-10-30 01:29:57 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8428</a>	0	None	None	None	2024-10-31 03:56:50 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8437</a>	0	None	None	None	2024-10-29 17:58:09 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8686</a>	0	None	None	None	2024-11-06 03:43:01 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8690</a>	0	None	None	None	2024-11-06 14:48:31 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8694</a>	0	None	None	None	2024-11-07 03:29:19 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8700</a>	0	None	None	None	2024-11-08 15:00:21 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8984</a>	0	None	None	None	2024-11-13 04:23:54 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:9051</a>	0	None	None	None	2024-11-11 01:27:18 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:9454</a>	0	None	None	None	2024-11-12 11:12:15 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:9459</a>	0	None	None	None	2024-11-12 11:13:20 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:9926</a>	0	None	None	None	2024-11-19 01:51:06 UTC
Red Hat Product Errata	<a href="#">RHSA-2025:0876</a>	0	None	None	None	2025-02-05 13:37:51 UTC
Red Hat	<a href="#">RHSA-2025:2454</a>	0	None	None	None	2025-03-13

Product Errata						05:47:04 UTC
Red Hat Product Errata	<a href="#">RHSA-2025:2710</a>	0	None	None	None	2025-03-19 20:55:08 UTC
Red Hat Product Errata	<a href="#">RHSA-2025:3301</a>	0	None	None	None	2025-04-03 00:21:39 UTC

OSIDB Bzimport  2024-10-09 03:04:42 UTC[Description](#)

A symlink traversal vulnerability in the containers/storage library can cause Podman, Buildah, and CRI-O to hang and potentially be DoSed via OOM kill when running a malicious image using an automatically assigned user namespace (`--userns=auto`` in Podman and Buildah). The containers/storage library will read `/etc/passwd` inside the container, but does not properly validate if that file is a symlink, which can be used to cause the library to read an arbitrary file on the host. This file is only read, and if it does not properly parse as a copy of `/etc/passwd`` it will cause an error (there is a small risk of information disclosure via the error message here as elements of the file that failed to parse can be included, but this is only as the user running Podman/Buildah/CRI-O so it wouldn't be a file they did not already have access to). The report here discovered that you can symlink `/etc/passwd` in the container to a FIFO on the host, causing a hang as the file cannot be completely read (or an OOM condition if the FIFO is continuously written to, which was then ready by Podman). This hang could occur in a critical section in the `c/storage` library, blocking other processes from creating containers, but could be easily solved via a SIGKILL of the affected process. The ability to potentially crash the CRI-O service via OOM kill could be more relevant, though the attacker would have to know the path of a FIFO that is regularly being written to on the host in order to do this.

errata-xmlrpc 2024-10-29 17:58:07 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via [RHSA-2024:8437](#) <https://access.redhat.com/errata/RHSA->

[2024:8437](#)

errata-xmlrpc 2024-10-30 01:29:56 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:8418 <https://access.redhat.com/errata/RHSA-2024:8418>

errata-xmlrpc 2024-10-31 03:56:48 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:8428 <https://access.redhat.com/errata/RHSA-2024:8428>

errata-xmlrpc 2024-11-06 03:42:59 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:8686 <https://access.redhat.com/errata/RHSA-2024:8686>

errata-xmlrpc 2024-11-06 14:48:29 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:8690 <https://access.redhat.com/errata/RHSA-2024:8690>

errata-xmlrpc 2024-11-07 03:29:17 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.12  
Ironic content for Red Hat OpenShift Container Platform 4.12

Via RHSA-2024:8694 <https://access.redhat.com/errata/RHSA-2024:8694>

errata-xmlrpc 2024-11-08 15:00:19 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:8700 <https://access.redhat.com/errata/RHSA-2024:8700>

errata-xmlrpc 2024-11-11 01:27:16 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:9051 <https://access.redhat.com/errata/RHSA-2024:9051>

errata-xmlrpc 2024-11-12 11:12:13 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:9454 <https://access.redhat.com/errata/RHSA-2024:9454>

errata-xmlrpc 2024-11-12 11:13:18 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:9459 <https://access.redhat.com/errata/RHSA-2024:9459>

errata-xmlrpc 2024-11-13 04:23:52 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via RHSA-2024:8984 <https://access.redhat.com/errata/RHSA-2024:8984>

errata-xmlrpc 2024-11-19 01:51:04 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2024:9926 <https://access.redhat.com/errata/RHSA-2024:9926>

errata-xmlrpc 2024-11-26 06:43:26 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:10289 <https://access.redhat.com/errata/RHSA-2024:10289>

errata-xmlrpc 2025-02-05 13:37:49 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via RHSA-2025:0876 <https://access.redhat.com/errata/RHSA-2025:0876>

errata-xmlrpc 2025-03-13 05:47:02 UTC

[Comment 19](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2025:2454 <https://access.redhat.com/errata/RHSA-2025:2454>

2025:2454

errata-xmlrpc 2025-03-19 20:55:06 UTC

[Comment 20](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2025:2710 <https://access.redhat.com/errata/RHSA-2025:2710>

errata-xmlrpc 2025-04-03 00:21:37 UTC

[Comment 21](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2025:3301 <https://access.redhat.com/errata/RHSA-2025:3301>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

