GitHub Advisory Database / Unreviewed / CVE-2024-9676

A vulnerability was found in Podman, Buildah, and CRI-O....

Moderate severity Unreviewed Published on Oct 15, 2024 to the GitHub Advisory Database • Updated on Mar 19

Package

No package listed— Suggest a package

Affected versions

Unknown

Patched versions

Unknown

Description

A vulnerability was found in Podman, Buildah, and CRI-O. A symlink traversal vulnerability in the containers/storage library can cause Podman, Buildah, and CRI-O to hang and result in a denial of service 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.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-9676
- https://access.redhat.com/security/cve/CVE-2024-9676
- https://bugzilla.redhat.com/show_bug.cgi?id=2317467
- GHSA-wq2p-5pc6-wpgf
- https://access.redhat.com/errata/RHSA-2024:8418
- https://access.redhat.com/errata/RHSA-2024:8437
- https://access.redhat.com/errata/RHSA-2024:8428
- https://access.redhat.com/errata/RHSA-2024:8686
- https://access.redhat.com/errata/RHSA-2024:8690
- https://access.redhat.com/errata/RHSA-2024:8694
- https://access.redhat.com/errata/RHSA-2024:8700
- https://access.redhat.com/errata/RHSA-2024:9051
- https://access.redhat.com/errata/RHSA-2024:9454
- https://access.redhat.com/errata/RHSA-2024:9459
- https://access.redhat.com/errata/RHSA-2024:8984
- https://access.redhat.com/errata/RHSA-2024:9926

- https://access.redhat.com/errata/RHSA-2024:10289
- https://access.redhat.com/errata/RHSA-2025:0876
- https://access.redhat.com/errata/RHSA-2025:2454
- https://access.redhat.com/errata/RHSA-2025:2710
- https://access.redhat.com/errata/RHSA-2025:3301
- containers/storage@ `935c58f`

Published by the National Vulnerability Database on Oct 15, 2024

Published to the GitHub Advisory Database on Oct 15, 2024

Last updated on Mar 19

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

EPSS score

1.276% (80th percentile)

Weaknesses

▶ CWE-22

CVE ID

CVE-2024-9676

GHSA ID

GHSA-wq2p-5pc6-wpgf

Source code

No known source code

Dependabot alerts are not supported on this advisory because it does not have a package from a supported ecosystem with an affected and fixed version.

Learn more about GitHub language support

Checking history

See something to contribute? Suggest improvements for this vulnerability.