



Red Hat Product Errata RHSA-2025:15904 - Security Advisory

RHSA-2025:15904 - Security Advisory

Issued: 2025-09-16 Updated: 2025-09-16

[Overview](#)[Updated Packages](#)

Synopsis

Important: container-tools:rhel8 security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

Topic

An update for the container-tools:rhel8 module is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

Description

The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.

Security Fix(es):

- podman: Podman kube play command may overwrite host files (CVE-2025-9566)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258>

Affected Products

- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

Fixes

- [BZ - 2393152](#) - CVE-2025-9566 podman: Podman kube play command may overwrite host files

CVEs

- [CVE-2025-9566](#)

References

- <https://access.redhat.com/security/updates/classification/#important>

The Red Hat security contact is secalert@redhat.com. More contact details at <https://access.redhat.com/security/team/contact/>.



Quick Links



Help



Site Info



Related Sites



 Partial system outage



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

All policies and guidelines

Digital accessibility

Cookie Preferences and Opt-Out Rights