

[Red Hat Product Errata](#) [RHSA-2025:7118 - Security Advisory](#)

RHSA-2025:7118 - Security Advisory

Issued: 2025-05-13 Updated: 2025-05-13

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

Synopsis

Important: osbuild and osbuild-composer 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 osbuild and osbuild-composer is now available for Red Hat Enterprise Linux 9.

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

A service for building customized OS artifacts, such as VM images and OSTree commits, that uses osbuild under the hood. Besides building images for local usage, it can also upload images directly to cloud. It is compatible with composer-cli and cockpit-composer clients.

Security Fix(es):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)
- go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion (CVE-2024-34158)
- golang-fips: Golang FIPS zeroed buffer (CVE-2024-9355)

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.

Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 9 Release Notes linked from 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 9 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x

Fixes

- BZ - 2262921  - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads
- BZ - 2310529  - CVE-2024-34158 go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion
- BZ - 2315719  - CVE-2024-9355 golang-fips: Golang FIPS zeroed buffer
- RHEL-56049  - Update Image Builder projects to their latest upstream releases [RHEL-9.6]
- RHEL-16396  - Image Builder: ability to customize LVM naming (VG and LV)

- [RHEL-4570](#) - RFE: Add custom filesystems especially ext4 - customers ask for this because ext4 can be shrunk while xfs cannot
- [RHEL-4617](#) - [RFE] Image Builder: advanced partitioning mode
- [RHEL-4636](#) - [RFE] ImageBuilder : Support custom swap partitioning in images
- [RHEL-78659](#) - Unexpected Warnings for User/Group Customizations Under [[customizations.files]]

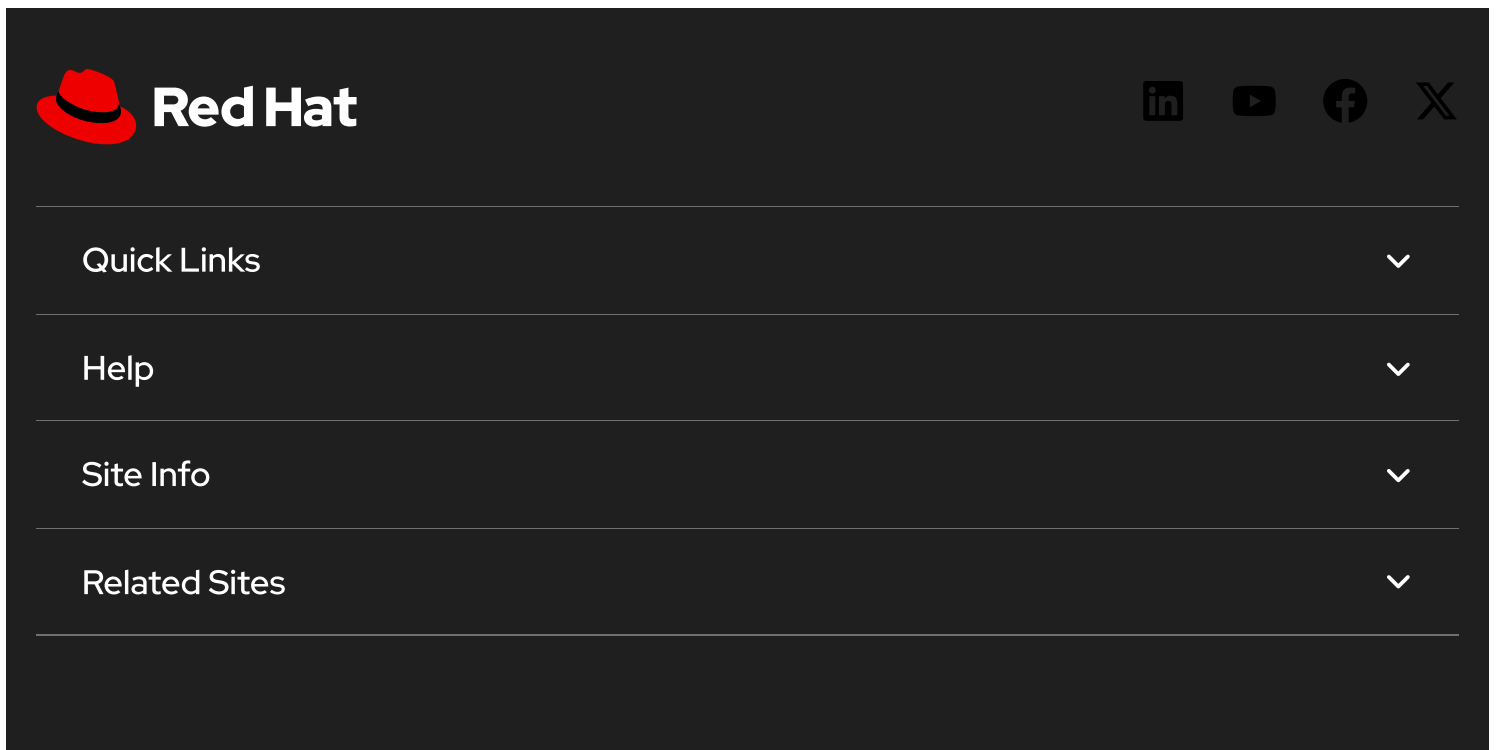
CVEs

- [CVE-2024-1394](#)
- [CVE-2024-9355](#)
- [CVE-2024-34158](#)

References

- <https://access.redhat.com/security/updates/classification/#important>
- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/9.6_release_notes/index

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



The image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat icon) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items: "Quick Links", "Help", "Site Info", and "Related Sites", each with a downward-pointing chevron icon to its right.

 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](#)