Red Hat F

RHSA
Advis

-05-06

Overview

Updated P

Synop

Moderat

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update for corosync is now available for Red Hat Enterprise Linux 9.4 Extended Update Support.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 corosync packages provide the Corosync Cluster Engine and C APIs for Red Hat Enterprise Linux cluster software.

Security Fix(es):

- corosync: Corosync: Denial of Service and information disclosure via crafted UDP packet (CVE-2026-35091)
- corosync: Corosync: Denial of Service via integer overflow in join message validation (CVE-2026-35092)

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 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux High Availability for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux Resilient Storage for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux Resilient Storage for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux High Availability for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux High Availability for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux High Availability for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux High Availability (for IBM z Systems) - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux High Availability (for ARM 64) - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Resilient Storage for IBM z Systems - Extended Update Support 9.4 s390x

- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux High Availability for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux High Availability for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux Resilient Storage for x86_64 - 4 years of updates 9.4 x86_64
- Red Hat Enterprise Linux Resilient Storage for Power, little endian - 4 years of updates 9.4 ppc64le
- Red Hat Enterprise Linux Resilient Storage for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64
- Red Hat Enterprise Linux High Availability for ARM 64 - Extended Life Cycle 9.4 aarch64
- Red Hat Enterprise Linux High Availability for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux High Availability for IBM z Systems - Extended Life Cycle 9.4 s390x
- Red Hat Enterprise Linux High Availability for x86_64 - Extended Life Cycle 9.4 x86_64
- Red Hat Enterprise Linux Resilient Storage for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux Resilient Storage for IBM z Systems - Extended Life Cycle 9.4 s390x
- Red Hat Enterprise Linux Resilient Storage for x86_64 - Extended Life Cycle 9.4 x86_64

Fixes

- BZ - 2453813 - CVE-2026-35091 corosync: Corosync: Denial of Service and information disclosure via crafted UDP packet
- BZ - 2453814 - CVE-2026-35092 corosync: Corosync: Denial of Service via integer overflow in join message validation

CVEs

- CVE-2026-35091
- CVE-2026-35092

References

- https://access.redhat.com/security/updates/classification/#moderate

---

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

Red Hat

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 Do Not Sell or Share My Personal Information