



Red Hat Product Errata    RHSA-2026:14216 - Security Advisory

# RHSA-2026:14216 - Security Advisory

Issued: 2026-05-06    Updated: 2026-05-06

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

## Synopsis

Moderate: corosync security update

## 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 8.8 Update Services for SAP Solutions and Red Hat Enterprise Linux 8.8 Telecommunications Update Service.

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 Extension 8.8 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.8 x86\_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux High Availability for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.8 x86\_64
- Red Hat Enterprise Linux High Availability for x86\_64 - Update Services for SAP Solutions 8.8 x86\_64
- Red Hat Enterprise Linux High Availability for x86\_64 - Telecommunications Update Service 8.8 x86\_64
- Red Hat Enterprise Linux High Availability for x86\_64 - Extended Update Support Extension 8.8 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

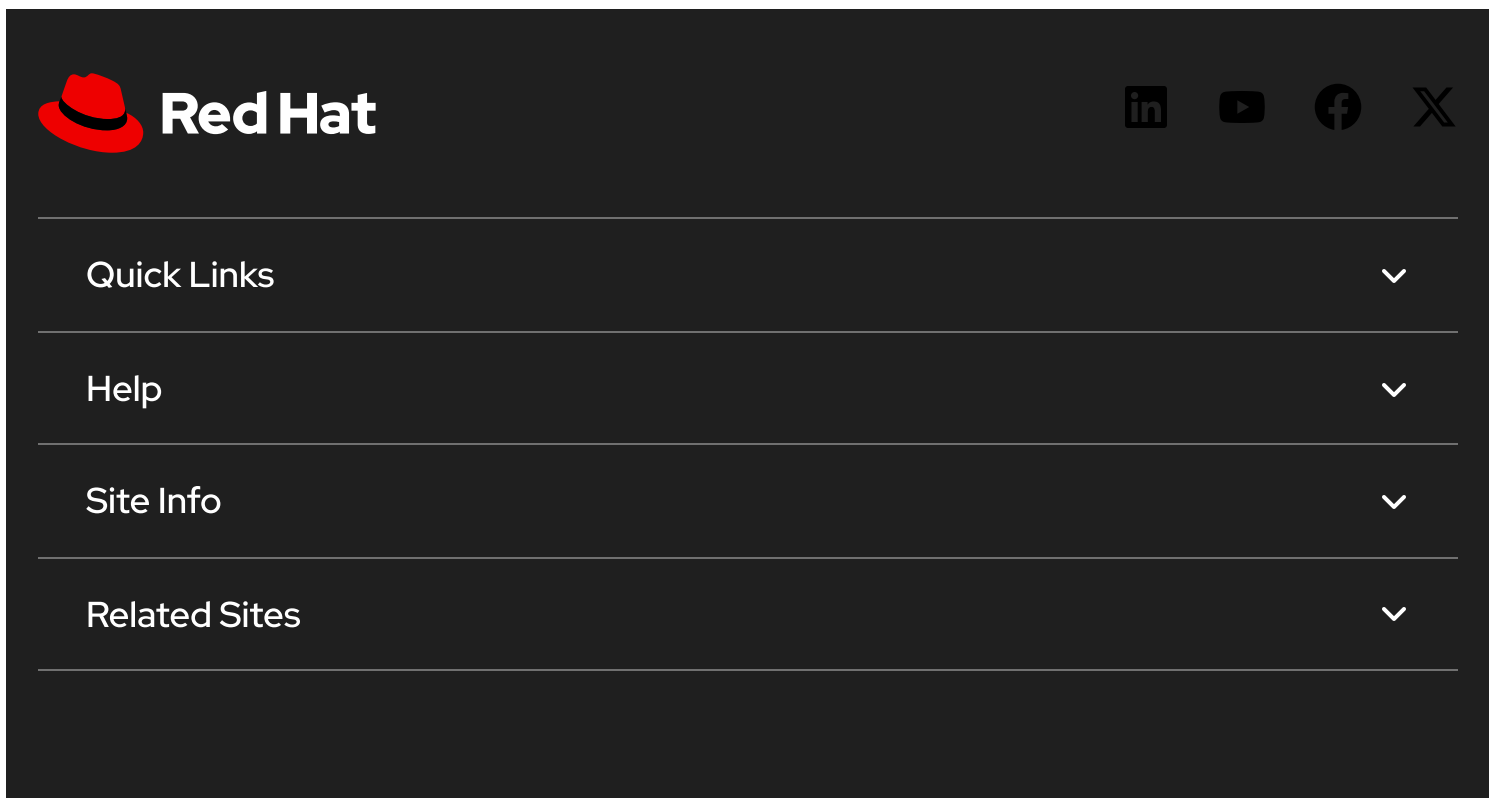
## CVEs

- [CVE-2026-35091](#)
- [CVE-2026-35092](#)


## References

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

The Red Hat security contact is [secalert@redhat.com](mailto: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) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items, each with a downward-pointing chevron icon: "Quick Links", "Help", "Site Info", and "Related Sites".

 Partial system outage



The image shows a dark-themed footer navigation area. On the left is a small icon of a grey hat. To its right are three links: "About Red Hat", "Jobs", and "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](#)