CVE-2026-35092

VEX

Public on April 1, 2026

Last modified: May 5, 2026 at 9:32:15 AM UTC

MODERATE

Moderate severity

What does this mean?

7.5

CVSS v3 Score Breakdown

Jump to section

Description Statement Mitigation Additional information Affected Packages CVSS Score Details Weakness (CWE) Acknowledgements FAQ

Description

A flaw was found in Corosync. An integer overflow vulnerability in Corosync's join message sanity validation allows a remote, unauthenticated attacker to send crafted User Datagram Protocol (UDP) packets. This can cause the service to crash, leading to a denial of service. This vulnerability specifically affects Corosync deployments configured to use totemudp/totemudpu mode.

Statement

This is an Important denial of service vulnerability in Corosync, affecting deployments configure d to use totemudp/totemudpu mode. A remote, unauthenticated attacker can send specially cr afted UDP packets to trigger an integer overflow, causing the Corosync service to crash.This iss ue affects Corosync only when using the legacy totemudp or totemudpu transports with unencr

ypted communication. These are not the default.The default transport is knet, which supports e ncryption and is the standard configuration in RHEL. The totemudp and totemudpu transports are unsupported in RHEL and require explicit manual configuration.

Mitigation

Restrict network access to Corosync cluster communication ports. Configure firewall rules to limit incoming UDP traffic to the Corosync service (default port 5405) to only trusted hosts within the cluster. This will prevent unauthenticated remote attackers from sending crafted packets to exploit the vulnerability. A service restart may be required for firewall changes to take full effect.

Additional information

- Bugzilla 2453814: corosync: Corosync: Denial of Service via integer overflow in join message validation
- CWE-190: Integer Overflow or Wraparound

External references

- https://www.cve.org/CVERecord?id=CVE-2026-35092
- https://nvd.nist.gov/vuln/detail/CVE-2026-35092
- https://bugzilla.redhat.com/show_bug.cgi?id=2453169

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	corosync
State	Fixed
Justification	None
Errata	RHSA-2026:13644
Release Date	May 5, 2026

Products / Services	Red Hat Enterprise Linux 10.0 Extended Update Support
Components	corosync
State	Fixed
Justification	None
Errata	RHSA-2026:14205
Release Date	May 6, 2026

Products / Services	Red Hat Enterprise Linux 8
Components	corosync
State	Fixed
Justification	None
Errata	RHSA-2026:13657

1 of 2

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	7.5	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	None	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	None	N/A	N/A
Integrity Impact	None	N/A	N/A
Availability Impact	High	N/A	N/A

CVSS v3 Vector

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

Acknowledgements

Red Hat would like to thank Sebastián Alba Vives for reporting this issue.

Frequently Asked Questions

- **Why is Red Hat's CVSS v3 score or Impact different from other vendors?**
- **My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?**
- **What can I do if my product is listed as "Will not fix"?**
- **What can I do if my product is listed as "Fix deferred"?**
- **What is a mitigation?**
- **I have a Red Hat product but it is not in the above list, is it affected?**
- **Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?**

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: May 5, 2026 at 9:32:15 AM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage