



Corosync: corosync: denial of service and information disclosure via crafted udp packet

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-35091 |
| State | PUBLISHED |
| Assigner | redhat |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-01 14:16:57 UTC |
| Updated | 2026-04-01 14:23:37 UTC |

Description A flaw was found in Corosync. A remote unauthenticated attacker can exploit a wrong return value vulnerability in the Corosync

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from secalert@redhat.com

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

Problem Types: CWE-253 | CWE-253 Incorrect Check of Function Return Value

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|---------|-------|----------|--|
| 3.1 | secalert@redhat.com | Primary | 8.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H |
| 3.1 | CNA | CVSS | 8.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

High

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------|--|---------------|---------------|
| CNA | Red Hat | Red Hat Enterprise Linux 10 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 7 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat OpenShift Container Platform 4 | Not specified | Not specified |

References

| Reference | Source | Link | Tags |
|---|---------------------|---|---------------------|
| bugzilla.redhat.com/show_bug.cgi | secalert@redhat.com | bugzilla.redhat.com | |
| bugzilla.redhat.com/show_bug.cgi | secalert@redhat.com | bugzilla.redhat.com | |
| access.redhat.com/security/cve/CVE-2026-35091 | secalert@redhat.com | access.redhat.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Sebastián Alba Vives for reporting this issue. (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|----------------------|
| CNA | 2026-04-01T11:31:01.742Z | Reported to Red Hat. |
| CNA | 2026-04-01T11:48:13.254Z | Made public. |

Workarounds

CNA: To mitigate this vulnerability, restrict network access to the Corosync service on UDP port 5405 to only trusted hosts or networks. If Corosync is not required, consider disabling the service. Example firewall rule to restrict access to a trusted network (replace <TRUSTED_NETWORK> with your network): ``firewall-cmd --permanent --add-rich-rule='rule family="ipv4" port port="5405" protocol="udp" source address="<TRUSTED_NETWORK>" accept`` ``firewall-cmd --reload`` To disable the Corosync service: ``systemctl stop corosync`` ``systemctl disable corosync`` Note that restricting access may impact cluster communication, and disabling the service will prevent cluster operation. A restart of the Corosync service or a

and disabling the service will prevent cluster operation. A restart of the CoreOS service or a system reboot may be required for changes to take full effect.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)