Corosync: corosync: denial of service via integer overflow in join message validation

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-35092
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. An integer overflow vulnerability in Corosync's join message sanity validation allows a remot

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

Problem Types: CWE-190 | CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/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	
access.redhat.com/security/cve/CVE-2026-35092	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.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	2026-04-01T11:32:04.388Z	Reported to Red Hat.
CNA	2026-04-01T11:48:22.309Z	Made public.

Workarounds

CNA: 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.

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