



# Llama-stack-k8s-operator: llama stack service exposed across namespaces due to missing networkpolicy

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

## Summary

<b>CVE</b>	CVE-2025-12805
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 22:16:25 UTC
<b>Updated</b>	2026-03-30 13:26:50 UTC

**Description** A flaw was found in Red Hat OpenShift AI (RHOAI) llama-stack-operator. This vulnerability allows unauthorized access to L

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from secalert@redhat.com

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

**EPSS:** 0.000340000 probability, percentile 0.097730000 (date 2026-04-01)

**Problem Types:** CWE-653 | CWE-653 Improper Isolation or Compartmentalization

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat OpenShift AI 2.25	unaffected sha256:c0d95dfbae20e87113ffb81026d379bb63ad300447df98b27d1bf9a83t
CNA	Red Hat	Red Hat OpenShift AI 2.25	unaffected sha256:1d258fe98c2477e4256a9b936f412f2501fb7ca9e3b810347f9712e0d5
CNA	Red Hat	Red Hat OpenShift AI RHOAI	Not specified
CNA	Red Hat	Red Hat OpenShift AI RHOAI	Not specified

### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/errata/RHSA-2026:2106">access.redhat.com/errata/RHSA-2026:2106</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://access.redhat.com/errata/RHSA-2026:2695">access.redhat.com/errata/RHSA-2026:2695</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	secalert@redhat.com	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
<a href="https://access.redhat.com/security/cve/CVE-2025-12805">access.redhat.com/security/cve/CVE-2025-12805</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

Source	Time	Event
CNA	2025-11-06T13:38:39.035Z	Reported to Red Hat.
CNA	2025-12-31T23:59:00.000Z	Made public.

### Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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](#)**