



Bug 2413101 (CVE-2025-12805) - CVE-2025-12805 llama-stack-k8s-operator: Llama Stack service exposed across namespaces due to missing NetworkPolicy

Keywords: Security

Reported: 2025-11-06 13:48 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-03 14:56 UTC ([History](#))

Alias: CVE-2025-12805

CC List: 3 users ([show](#))

Deadline: 2025-12-31

Product: Security Response

Fixed In Version:

Clone Of:

Component: vulnerability

Environment:

Last Closed:

Embargoed:

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2025-11-06 13:48:11 UTC

[Description](#)

I've found something that looks like a security bug related to llama-stack and llama-stack-operator, affecting RHOAI 2.24 and RHOAI 2.25:

When UserA creates a LlamaStackDistribution in a namespace, a service is created. Using a notebook, UserA can use the llama_stack_client SDK with the service endpoint. The service is not secured by any Network Policy. UserB, running a notebook in a different namespace, can also query UserA's llama-stack service just having the endpoint, which is easy to guess. I think the llama-stack-operator should add a NetworkPolicy

protecting the llama-stack service, so only pods in the same namespace can access to it. I believe rhods-dashboard in redhat-ods-applications also needs to be able to access it for RHOAI 3.0

I'll create now a bug in Jira to track this. Do you agree that this is a bug? Or users need to enable authentication to protect the llama-stack service?

Found in build:

rhoai-2.25 nightly build: 2025-10-01T06:19:17

How to reproduce:

As UserA, create a data science project, create a LlamaStackDistribution, start a workbench and run the attached notebook vector-stores-create-file (modifying the endpoint)

As UserB, create a data science project, start a workbench and run the attached notebook vector-stores-list-contents (modifying the endpoint). Verify that able to access UserA's information

Note

You need to [log in](#) before you can comment on or make changes to this bug.

