



Bug 2405966 (CVE-2025-12103) - CVE-2025-12103 openshift-ai: Trusty AI Grants All Authenticated users to list pods in any namespace

Keywords: Security

Reported: 2025-10-23 02:56 UTC by OSIDB Bzimport

Status: NEW

Modified: 2025-10-28 13:23 UTC ([History](#))

Alias: CVE-2025-12103

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

Deadline: 2025-10-28

Fixed In Version:

Product: Security Response

Clone Of:

Component: vulnerability

Environment:

Last Closed:

Embargoed:

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

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

Attachments ([Terms of Use](#))

OSIDB Bzimport 2025-10-23 02:56:10 UTC	Description
	A flaw was found in Openshift AI. The TrustyAI component is granting all service accounts and users on a cluster permissions to get, list, watch any pod in any namespace on the cluster.

Note

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

