



Openshift-ai: trusty ai grants all authenticated users to list pods in any namespace

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

Summary

CVE	CVE-2025-12103
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-28 14:15:55 UTC
Updated	2026-04-23 18:16:22 UTC

Description A flaw was found in Red Hat Openshift AI Service. The TrustyAI component is granting all service accounts and users on a

Risk And Classification

Primary CVSS: v3.1 5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000340000 probability, percentile 0.098480000 (date 2026-04-24)

Problem Types: CWE-266 | CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat OpenShift AI 2.25	unaffected sha256:6503aa2b0c29d01b947b6fde383850d03dcb2b9f9d70cf417b9e90d5e
CNA	Red Hat	Red Hat OpenShift AI 3	unaffected sha256:2015d93a8f499c4b3706fb1b1323db2e455154cb20219ceef82b79894
CNA	Red Hat	Red Hat OpenShift AI RHOAI	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-2025-12103	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:10184	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21117	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-10-23T02:53:02.820Z	Reported to Red Hat.
CNA	2025-10-28T09:00:00.000Z	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.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report