Odh-dashboard: odh dashboard kubernetes service account exposure

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5483
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 18:16:46 UTC
Updated	2026-04-10 21:16:28 UTC
Description	A flaw was found in odh-dashboard in Red Hat Openshift AI. This vulnerability in the `odh-dashboard` component of Red H

Risk And Classification

Primary CVSS: v3.1 8.5 HIGH from secalert@redhat.com

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

Problem Types: CWE-201 | CWE-201 Insertion of Sensitive Information Into Sent Data

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	8.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
High

Privileges Required
Low

User Interaction
None

Scope
Changed

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat OpenShift AI 2.16	unaffected sha256:0a983da3de4ce816435e23da23c4b6f373008aaf2df2b9820bdcc77a9
CNA	Red Hat	Red Hat OpenShift AI 2.25	unaffected sha256:15ee3fb5fedf759e82c8de8020da1931c9de8138737f1cc7cf6622847a
CNA	Red Hat	Red Hat OpenShift AI 3.2	unaffected sha256:0bdb9912d41d799b0237fe75f3fdc843983ab4ebfe6b5a47f7d4a00a64
CNA	Red Hat	Red Hat OpenShift AI 3.3	unaffected sha256:14ee2bbd445b8a988c487d4b4a7b02ff9afe1c07034b4bba073a5a826
CNA	Red Hat	Red Hat OpenShift AI RHOAI	Not specified
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
access.redhat.com/errata/RHSA-2026:7403	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7398	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7397	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-5483	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7404	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	2026-04-03T00:00:00.000Z	Reported to Red Hat.
CNA	2026-04-10T17:16:00.000Z	Made public.

Workarounds

CNA: If applying the update is not immediately possible, the vulnerability can be mitigated by disabling or removing the NIM (NVIDIA Inference Microservice) integration from the Red Hat OpenShift AI (RHOAI) environment.

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

Free CVE JSON API cve.report/api

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