



## Bug 2454764 (CVE-2026-5483) - CVE-2026-5483 odh-dashboard: ODH Dashboard Kubernetes Service Account Exposure

**Keywords:** Security

**Reported:** 2026-04-03 12:49 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-04-10 17:26 UTC ([History](#))

**Alias:** CVE-2026-5483

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

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** high

**Severity:** high

**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 2026-04-03 12:49:02 UTC

[Description](#)

A flaw was found in odh-dashboard in Red Hat Openshift AI. This vulnerability in the `odh-dashboard` component of Red Hat OpenShift AI (RHOAI) allows for the disclosure of Kubernetes Service Account tokens through a NodeJS endpoint. This could enable an attacker to gain unauthorized access to Kubernetes resources.

Note

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

