Bug 2463152 (CVE-2026-7163) - CVE-2026-7163 assisted-service: assisted-service: Authenticated users can gain administrative access to OpenShift clusters via credential disclosure

Keywords: Security

Status: NEW

Alias: CVE-2026-7163

Deadline: 2026-04-30

Product: Security Response

Component: vulnerability

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

Reported: 2026-04-27 04:21 UTC by OSIDB Bzimport

Modified: 2026-04-30 12:04 UTC (History)

CC List: 6 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-27 04:21:20 UTC Description

```
A vulnerability in the assisted-service REST API, an optional
Assisted Installer (assisted-service) component in the
Multicluster Engine (MCE), allows an authenticated user with
minimal namespace-scoped privileges to obtain administrative
credentials for arbitrary clusters provisioned through the
hub.

The credentials download endpoint (GET
/v2/clusters/{cluster_id}/credentials, which returns the
kubeadmin password) and the kubeconfig download endpoint are
operational in AUTH_TYPE=local mode, the only authentication
```

mode available in on-premises ACM/MCE hub deployments. The local authenticator unconditionally grants full administrative access to any request bearing a valid JWT, with no per-endpoint restrictions. A valid local JWT is embedded as a plaintext query parameter in InfraEnvStatus.ISODownloadURL and is readable by any user who has get rights on an InfraEnv object in their own namespace.

The affected components ship as part of Multicluster Engine (MCE). The Red Hat Advanced Cluster Management (ACM) deployments that include MCE are equally affected.
This issue does not affect the hosted SaaS offering (console.redhat.com), which uses a different authentication mode.

Successful exploitation gives the attacker the kubeadmin password and kubeconfig for any OpenShift cluster provisioned through the affected hub, granting unrestricted root-level administrative access to those spoke clusters.

Note

You need to log in before you can comment on or make changes to this bug.