Assisted-service: assisted-service: authenticated users can gain administrative access to openshift clusters via credential disclosure

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

Summary

CVE	CVE-2026-7163
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 14:16:36 UTC
Updated	2026-04-30 22:16:26 UTC
Description	A vulnerability in the assisted-service REST API, an optional Assisted Installer (assisted-service) component in the Multiclu

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-312 | CWE-312 Cleartext Storage of Sensitive Information

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Adjacent

Attack Complexity
Low

Privileges Required
Low

User Interaction
Required

Scope
Changed

Confidentiality
High

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Multicluster Engine For Kubernetes 2.1	unaffected 1776983527 * rpm	Not specified
CNA	Red Hat	Multicluster Engine For Kubernetes 2.11	unaffected 1776987609 * rpm	Not specified
CNA	Red Hat	Multicluster Engine For Kubernetes 2.7	unaffected 1777205801 * rpm	Not specified
CNA	Red Hat	Multicluster Engine For Kubernetes 2.7	unaffected 1777205772 * rpm	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:12337	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11511	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11512	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-7163	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2026:12116	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: This issue was discovered by Nick Carboni (Red Hat), Omer Vishlitzky (Red Hat), and Riccardo Piccoli (Red Hat). (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-27T04:18:06.534Z	Reported to Red Hat.
CNA	2026-04-30T12:00:00.000Z	Made public.

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