



# 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

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

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from [secalert@redhat.com](mailto: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	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	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

Integrity

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	<a href="#">Multicluster Engine For Kubernetes 2.1</a>	unaffected 1776983527 * rpm	Not specified
CNA	Red Hat	<a href="#">Multicluster Engine For Kubernetes 2.11</a>	unaffected 1776987609 * rpm	Not specified
CNA	Red Hat	<a href="#">Multicluster Engine For Kubernetes 2.7</a>	unaffected 1777205801 * rpm	Not specified
CNA	Red Hat	<a href="#">Multicluster Engine For Kubernetes 2.7</a>	unaffected 1777205772 * rpm	Not specified

#### References

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)