



# Helm impersonation bypass of `RESTClientGetter` retains `cluster-admin` during template rendering

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-41050
<b>State</b>	PUBLISHED
<b>Assigner</b>	suse
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-13 08:16:16 UTC
<b>Updated</b>	2026-05-13 15:35:35 UTC
<b>Description</b>	Fleet's Helm deployer did not fully apply ServiceAccount impersonation in two code paths, allowing a tenant with git push a

## Risk And Classification

**Primary CVSS:** v3.1 9.9 CRITICAL from meissner@suse.de

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

**EPSS:** 0.000390000 probability, percentile 0.117630000 (date 2026-05-14)

**Problem Types:** CWE-863 | CWE-863 CWE-863: Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	meissner@suse.de	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SUSE	Rancher	affected 0.15.0 0.15.1 semver	Not specified
CNA	SUSE	Rancher	affected 0.14.0 0.14.5 semver	Not specified
CNA	SUSE	Rancher	affected 0.13.0 0.13.10 semver	Not specified
CNA	SUSE	Rancher	affected 0.12.0 0.12.14 semver	Not specified
CNA	SUSE	Rancher	affected 0.11.0 0.11.13 semver	Not specified

### References

Reference	Source	Link	Tags
bugzilla.suse.com/show_bug.cgi	meissner@suse.de	bugzilla.suse.com	
github.com/advisories/GHSA-765j-qfrp-hm3j	meissner@suse.de	github.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:** <https://github.com/kodareef5> (en)

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)