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

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

Summary

CVE	CVE-2026-41050
State	PUBLISHED
Assigner	suse
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 08:16:16 UTC
Updated	2026-05-13 15:35:35 UTC
Description	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

ntegrity

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.