



Juju CloudSpec API could leak sensitive information

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-5412
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 13:16:45 UTC
Updated	2026-04-13 15:02:06 UTC
Description	In Juju versions prior to 2.9.57 and 3.6.21, an authorization issue exists in the Controller facade. An authenticated user can

Risk And Classification

Primary CVSS: v3.1 9.9 CRITICAL from security@ubuntu.com

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

EPSS: 0.000370000 probability, percentile 0.109080000 (date 2026-04-15)

Problem Types: CWE-285 | CWE-285 CWE-285: Improper Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security@ubuntu.com	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

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	Canonical	Juju	affected 2.9.0 2.9.57 semver	Linux
CNA	Canonical	Juju	affected 3.6.0 3.6.21 semver	Linux

References

Reference	Source	Link	Tags
github.com/juju/juju/pull/22205	security@ubuntu.com	github.com	
github.com/juju/juju/pull/22206	security@ubuntu.com	github.com	
github.com/juju/juju/security/advisories/GHSA-w5fq-8965-c969	security@ubuntu.com	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: [Ales Stimec \(en\)](#)

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

CVE.report and Source URL Uptime Status status.cve.report