



# CVE-2026-40213

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

## Summary

<b>CVE</b>	CVE-2026-40213
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 22:16:34 UTC
<b>Updated</b>	2026-05-07 22:16:34 UTC
<b>Description</b>	OpenStack Cyborg before 16.0.1 uses rule:allow (check_str='@') as the default policy for multiple API endpoints. This unco

## Risk And Classification

**Primary CVSS:** v3.1 7.4 HIGH from cve@mitre.org

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

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

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	Secondary	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">OpenStack</a>	<a href="#">Cyborg</a>	affected 5.0.0 14.0.1 semver	Not specified
CNA	<a href="#">OpenStack</a>	<a href="#">Cyborg</a>	affected 15.0.0 15.0.1 semver	Not specified
CNA	<a href="#">OpenStack</a>	<a href="#">Cyborg</a>	affected 16.0.0 16.0.1 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.openwall.com/lists/oss-security/2026/05/07/6">www.openwall.com/lists/oss-security/2026/05/07/6</a>	<a href="mailto:cve@mitre.org">cve@mitre.org</a>	<a href="http://www.openwall.com">www.openwall.com</a>	
<a href="https://bugs.launchpad.net/openstack-cyborg/+bug/2143263">bugs.launchpad.net/openstack-cyborg/+bug/2143263</a>	<a href="mailto:cve@mitre.org">cve@mitre.org</a>	<a href="https://bugs.launchpad.net">bugs.launchpad.net</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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)