



# runZero Platform incorrect credential scope

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

## Summary

<b>CVE</b>	CVE-2026-5384
<b>State</b>	PUBLISHED
<b>Assigner</b>	runZero
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-07 15:17:48 UTC
<b>Updated</b>	2026-04-21 15:40:40 UTC
<b>Description</b>	An issue that could allow a credential to be updated and used for a task from outside of the authorized organization scope for

## Risk And Classification

**Primary CVSS:** v3.1 5.8 MEDIUM from 44488dab-36db-4358-99f9-bc116477f914

**CVSS:** [3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N](#)

**EPSS:** 0.000440000 probability, percentile 0.135670000 (date 2026-04-22)

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

Version	Source	Type	Score	Severity	Vector
3.1	44488dab-36db-4358-99f9-bc116477f914	Secondary	5.8	MEDIUM	<a href="#">CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N</a>
3.1	CNA	CVSS	5.8	MEDIUM	<a href="#">CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N</a>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**High**

User Interaction

**None**

Scope

**Changed**

Confidentiality

**High**

Integrity

**None**

None  
Availability  
None  
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Runzero	Runzero Platform	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	RunZero	Platform	affected 4.0.26021.0 semver	Not specified

### References

Reference	Source	Link	Tags
www.runzero.com/advisories/runzero-platform-cve-2026-5384	44488dab-36db-4358-99f9-bc116477f914	<a href="http://www.runzero.com">www.runzero.com</a>	Vendor Adv
help.runzero.com/docs/release-notes	44488dab-36db-4358-99f9-bc116477f914	<a href="http://help.runzero.com">help.runzero.com</a>	Release No
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

### Vendor Comments And Credit

Discovery Credit  
**CNA:** runZero (en)

### Additional Advisory Data

Solutions  
**CNA:** This issue was fixed in version 4.0.26021.0 of the runZero Platform

There are currently no legacy QID mappings associated with this CVE.

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)