



# runZero Platform MCP certification information leak

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

## Summary

<b>CVE</b>	CVE-2026-5379
<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 15:17:47 UTC
<b>Updated</b>	2026-04-21 15:33:01 UTC
<b>Description</b>	An issue that allowed MCP agents to access certificate information from outside of their authorized organization scope has

## Risk And Classification

**Primary CVSS:** v3.1 3 LOW from 44488dab-36db-4358-99f9-bc116477f914

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

**EPSS:** 0.000230000 probability, percentile 0.061970000 (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	3	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	3	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

None

None  
Availability  
None  
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/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 4.0.260203.0 semver	Not specified

### References

Reference	Source	Link
help.runzero.com/docs/release-notes	44488dab-36db-4358-99f9-bc116477f914	<a href="https://help.runzero.com/docs/release-notes">help.runzero.c</a>
www.runzero.com/advisories/runzero-platform-mcp-cert-infoleak-cve-2026-5379	44488dab-36db-4358-99f9-bc116477f914	<a href="https://www.runzero.com/advisories/runzero-platform-mcp-cert-infoleak-cve-2026-5379">www.runzero.c</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

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

### Additional Advisory Data

Solutions  
**CNA:** This issue was fixed in version 4.0.260203.0 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)