runZero Platform MCP information leak

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

Summary

CVE	CVE-2026-5374
State	PUBLISHED
Assigner	runZero
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 15:17:47 UTC
Updated	2026-04-21 15:10:18 UTC
Description	An issue that allowed MCP agents to access remediation and asset information from outside of the authorized organization

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	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	5.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N

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 4.0.260202.0 semver	Not specified

References

Reference	Source	Link
www.runzero.com/advisories/runzero-platform-mcp-infoleak-cve-2026-5374	44488dab-36db-4358-99f9-bc116477f914	www.runzero.com
help.runzero.com/docs/release-notes	44488dab-36db-4358-99f9-bc116477f914	help.runzero.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: runZero (en)

Additional Advisory Data

Solutions

CNA: This issue was fixed in version 4.0.260202.0 of the runZero Platform

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

Free CVE JSON API cve.report/api

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