



# runZero Platform SQL injection in saved queries

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-5372
<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 15:17:46 UTC
<b>Updated</b>	2026-04-21 15:06:58 UTC
<b>Description</b>	An issue that allowed a SQL injection attack vector related to saved queries (introduced in version 4.0.260123.0). This is ar

## Risk And Classification

**Primary CVSS:** v3.1 6.4 MEDIUM from 44488dab-36db-4358-99f9-bc116477f914

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

**EPSS:** 0.000350000 probability, percentile 0.103580000 (date 2026-04-22)

**Problem Types:** CWE-89 | CWE-89 CWE-89 Improper neutralization of special elements used in an SQL command ('SQL injection')

Version	Source	Type	Score	Severity	Vector
3.1	44488dab-36db-4358-99f9-bc116477f914	Secondary	6.4	MEDIUM	<a href="#">CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H</a>
3.1	CNA	CVSS	6.4	MEDIUM	<a href="#">CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H</a>

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Runzero	Runzero Platform	4.0.260123.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	RunZero	Platform	affected 4.0.260123.0 4.0.260123.1 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.com</a>
www.runzero.com/advisories/runzero-platform-saved-sqli-cve-2026-5372	44488dab-36db-4358-99f9-bc116477f914	<a href="https://www.runzero.com/advisories/runzero-platform-saved-sqli-cve-2026-5372">www.runzero.com</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 4.0.260123.1 of the runZero Platform

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)