



# CVE-2026-29953

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-29953  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | mitre   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-03-30 16:16:04 UTC   |
| <b>Updated</b>         | 2026-04-02 20:10:42 UTC   |
| <b>Description</b>     | SQL Injection vulnerability in SchemaHero 0.23.0 via the column parameter to the columnAsInsert function in file plugins/p... |

## Risk And Classification

**Primary CVSS:** v3.1 7.4 HIGH from ADP

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

**EPSS:** 0.000260000 probability, percentile 0.072780000 (date 2026-04-02)

**Problem Types:** CWE-89 | n/a | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1     | ADP                                  | DECLARED  | 7.4   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 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

#### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product    | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| Application | Schemahero | Schemahero | All     | All    | All     | All      |

#### Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

#### References

| Reference  | Source        | Link  | Tags                          |
|--|---------------|---|-------------------------------|
| github.com/b0b0haha/SchemaHero--Sqlinjection/blob/main/README.md | cve@mitre.org | <a href="https://github.com">github.com</a>           | Exploit, Third Party Advisory |
| gist.github.com/b0b0haha/fb59199fb1fdf9414e76442e0599bfed        | cve@mitre.org | <a href="https://gist.github.com">gist.github.com</a> | Exploit, Third Party Advisory |
| CVE Program record   | CVE.ORG       | <a href="https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)