



# Improper Access Control in Data Model Acceleration in Splunk Enterprise

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

## Summary

<b>CVE</b>	CVE-2026-20203
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisco
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 16:16:34 UTC
<b>Updated</b>	2026-04-17 19:07:27 UTC
<b>Description</b>	In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.260

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from psirt@cisco.com

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

**EPSS:** 0.000280000 probability, percentile 0.077230000 (date 2026-04-20)

**Problem Types:** CWE-284 | CWE-284 The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Splunk	Splunk Enterprise	affected 10.2 10.2.2 custom	Not specified
CNA	Splunk	Splunk Enterprise	affected 10.0 10.0.5 custom	Not specified
CNA	Splunk	Splunk Enterprise	affected 9.4 9.4.10 custom	Not specified
CNA	Splunk	Splunk Enterprise	affected 9.3 9.3.11 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.4.2603 Not Affected custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.3.2512 10.3.2512.6 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.2.2510 10.2.2510.10 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.1.2507 10.1.2507.19 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.0.2503 10.0.2503.13 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 9.3.2411 9.3.2411.127 custom	Not specified

### References

Reference	Source	Link	Tags
<a href="https://advisory.splunk.com/advisories/SVD-2026-0402">advisory.splunk.com/advisories/SVD-2026-0402</a>	psirt@cisco.com	<a href="https://advisory.splunk.com">advisory.splunk.com</a>	Vendor 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

### Vendor Comments And Credit

Discovery Credit

**CNA:** Mr Hack (try\_to\_hack) Santiago Lopez (en)

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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)