



# Sensitive Information Disclosure in "\_internal" index in Splunk MCP Server app

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

## Summary

<b>CVE</b>	CVE-2026-20205
<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 15:09:46 UTC
<b>Description</b>	In Splunk MCP Server app versions below 1.0.3 , a user who holds a role with access to the Splunk `_internal` index or pos

## Risk And Classification

**Primary CVSS:** v3.1 7.2 HIGH from psirt@cisco.com

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

**EPSS:** 0.000390000 probability, percentile 0.116050000 (date 2026-04-20)

**Problem Types:** CWE-532 | CWE-532 Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Splunk</a>	<a href="#">Splunk MCP Server</a>	affected 1.0 1.0.3 custom	Not specified

### References

Reference	Source	Link	Tags
<a href="https://advisory.splunk.com/advisories/SVD-2026-0407">advisory.splunk.com/advisories/SVD-2026-0407</a>	psirt@cisco.com	<a href="https://advisory.splunk.com">advisory.splunk.com</a>	
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:** [Charlie Huggard, Splunk \(en\)](#)

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](https://cve.report/api)

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