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

Advisory ID: SVD-2026-0407

CVE ID: CVE-2026-20205 (https://www.cve.org/CVERecord?id=CVE-2026-20205)

Published: 2026-04-15

Last Update: 2026-04-15

CVSSv3.1 Score: 7.2, High

CVSSv3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H (https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE: CWE-532 (https://cwe.mitre.org/data/definitions/532.

Bug ID: VULN-64757

Description

In Splunk MCP Server app versions below 1.0.3 , a user who holds a role with access to the Splunk `_internal` index or possesses the high-privilege capability `mcp_tool_admin` could view users session and authorization tokens in clear text.

The vulnerability would require either local access to the log files or administrative access to internal indexes, which by default only the admin role receives.

Review roles and capabilities on your instance and restrict internal index access to administrator-level roles. See Define roles on the Splunk platform with capabilities (https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities) and Connecting to

MCP Server and Admin settings (https://help.splunk.com/en/splunk-enterprise/mcp-server-for-splunk-platform/connecting-to-mcp-server-and-admin-settings) in the Splunk documentation for more information.

Solution

Upgrade Splunk MCP Server app to version 1.0.3, or higher.

Product Status

Product	Base Version	Component	Affected Version	Fix Version
Splunk MCP Server	1.0	-	Below 1.0.3	1.0.3

Mitigations and Workarounds

None

Detections

None

Severity

Splunk rates this vulnerability a 7.2, High, with a CVSSv3.1 vector of CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H.

If you do not use and have never installed Splunk MCP Server app, there should be no impact and the severity would be informational.

Acknowledgments

Charlie Huggard, Splunk