



# Flowise: Authenticated RCE Via MCP Adapters

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

## Summary

<b>CVE</b>	CVE-2026-40933
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 22:16:19 UTC
<b>Updated</b>	2026-04-22 14:17:03 UTC
<b>Description</b>	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, due to unsafe seriali

## Risk And Classification

**Primary CVSS:** v3.1 9.9 CRITICAL from security-advisories@github.com

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

**Problem Types:** CWE-78 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.9	CRITICAL	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H</b>
3.1	CNA	DECLARED	10	CRITICAL	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Changed**

Confidentiality

**High**

Integrity

**High**

Availability

High

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">FlowiseAI</a>	<a href="#">Flowise</a>	affected < 3.1.0	Not specified
CNA	<a href="#">FlowiseAI</a>	<a href="#">Flowise-components</a>	affected < 3.1.0	Not specified

#### References

Reference	Source	Link
<a href="https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-c9gw-hvqq-f33r">github.com/FlowiseAI/Flowise/security/advisories/GHSA-c9gw-hvqq-f33r</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>
<a href="https://www.ox.security/blog/the-mother-of-all-ai-supply-chains-critical-systemic-vul...">www.ox.security/blog/the-mother-of-all-ai-supply-chains-critical-systemic-vul...</a>	security-advisories@github.com	<a href="https://www.ox.security">www.ox.securi</a>
<a href="https://www.ox.security/blog/mcp-supply-chain-advisory-rce-vulnerabilities-across-the...">www.ox.security/blog/mcp-supply-chain-advisory-rce-vulnerabilities-across-the...</a>	security-advisories@github.com	<a href="https://www.ox.security">www.ox.securi</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>

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](#) 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)