n8n-MCP: Authenticated SSRF in n8n-mcp webhook and API client paths

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-44694
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 20:16:31 UTC
Updated	2026-05-08 20:16:31 UTC
Description	n8n-MCP is an MCP server that provides AI assistants access to n8n node documentation, properties, and operations. Fror

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000330000 probability, percentile 0.096560000 (date 2026-05-11)

Problem Types: CWE-367 | CWE-918 | CWE-367 CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:H/SI
4.0	CNA	DECLARED	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:H/SI

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

Low

Availability

Low

Sub Conf.

High

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Czlonkowski	N8n-mcp	affected >= 2.18.7, < 2.50.2	Not specified

References

Reference	Source	Link	Ta
github.com/czlonkowski/n8n-mcp/releases/tag/v2.50.2	security-advisories@github.com	github.com	
github.com/czlonkowski/n8n-mcp/security/advisories/GHSA-cmrh-wvq6-wm9r	security-advisories@github.com	github.com	
github.com/czlonkowski/n8n-mcp/commit/bcaba839409d470abeb4a6ad9b361b553a...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report