n8n: XSS via MCP OAuth client

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

Summary

CVE	CVE-2026-42235
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 19:16:06 UTC
Updated	2026-05-06 18:05:44 UTC
Description	n8n is an open source workflow automation platform. Prior to versions 1.123.32, 2.17.4, and 2.18.1, an unauthenticated atta

Risk And Classification

Primary CVSS: v4.0 8.8 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:L/SC:H/SI:H/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: 0.000910000 probability, percentile 0.253280000 (date 2026-05-05)

Problem Types: CWE-79 | CWE-87 | CWE-87 CWE-87: Improper Neutralization of Alternate XSS Syntax | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:L/SC:H/
4.0	CNA	DECLARED	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:L/SC:H/
3.1	nvd@nist.gov	Primary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:L/SC:H/SI:H/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	N8n	N8n	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	N8n-io	N8n	affected < 1.123.32	Not specified
CNA	N8n-io	N8n	affected >= 2.17.0, < 2.17.4	Not specified
CNA	N8n-io	N8n	affected >= 2.18.0, < 2.18.1	Not specified

References

Reference	Source	Link	Tags
github.com/n8n-io/n8n/security/advisories/GHSA-537j-gqpc-p7fq	security-advisories@github.com	github.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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