Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0049

Kwetsbaarheden verholpen in n8n

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-02-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

n8n heeft kwetsbaarheden verholpen in versies 1.114.3, 1.115.0, 1.123.17, 2.5.2, 1.122.5, 1.123.2, 1.123.18, 2.5.0, 1.123.10, 2.5.0, 2.2.1, 1.123.9, 1.123.12, 2.4.0, 1.118.0, 2.4.0, 2.4.8, en 1.120.3.

Duiding

De kwetsbaarheden omvatten onder andere het gebruik van `Buffer.allocUnsafe()` en `Buffer.allocUnsafeSlow()`, wat kan leiden tot informatie openbaarmaking. Daarnaast zijn er kwetsbaarheden in de expressie-evaluatiefuncties die geauthenticeerde gebruikers in staat stellen om ongewenste systeemcommando's uit te voeren. Er zijn ook Cross-site Scripting (XSS) kwetsbaarheden ontdekt in de webhook-responsverwerking en de markdown-renderingcomponent, die kunnen leiden tot sessieovername. Verder zijn er kwetsbaarheden in de bestandsaccesscontrols en de Git-node, die het mogelijk maken voor geauthenticeerde gebruikers om gevoelige bestanden te lezen en willekeurige commando's uit te voeren. Een andere kwetsbaarheid stelt ongeauthenticeerde aanvallers in staat om workflows te exploiteren die geüploade bestanden via SSH verwerken, wat kan leiden tot remote code execution. Bovendien is er een kwetsbaarheid in de Merge-node's SQL Query-modus, en in de Python Code-node die het mogelijk maakt om de sandbox-omgeving te ontsnappen. Tot slot is er een command injection-kwetsbaarheid in de community package installatie.

Oplossingen

n8n heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/advisories/GHSA-49mx-fj45-q3p6
- https://github.com/advisories/GHSA-6cqr-8cfr-67f8
- https://github.com/advisories/GHSA-7c4h-vh2m-743m
- https://github.com/advisories/GHSA-825q-w924-xhgx
- https://github.com/advisories/GHSA-8398-gmmx-564h
- https://github.com/advisories/GHSA-9g95-qf3f-ggrw
- https://github.com/advisories/GHSA-gfvg-qv54-r4pc
- https://github.com/advisories/GHSA-hv53-3329-vmrm
- https://github.com/advisories/GHSA-m82q-59gv-mcr9
- https://github.com/advisories/GHSA-qpq4-pw7f-pp8w

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-61917	7.7 HIGH
CVE-2026-25049	9.4 CRITICAL
CVE-2026-25051	8.5 HIGH
CVE-2026-25052	9.4 CRITICAL
CVE-2026-25053	9.4 CRITICAL
CVE-2026-25054	8.5 HIGH
CVE-2026-25055	7.1 HIGH
CVE-2026-25056	9.4 CRITICAL
CVE-2026-25115	9.4 CRITICAL
CVE-2026-21893	9.4 CRITICAL

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition

CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-668	Exposure of Resource to Wrong Sphere
CWE-693	Protection Mechanism Failure
CWE-913	Improper Control of Dynamically-Managed Code Resources

Getroffen producten

N8N
N8N

Disclaimer