Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0228

Kwetsbaarheden verholpen in n8n workflow automation platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-07-2026

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 meerdere kwetsbaarheden verholpen in het n8n workflow automation platform.

Duiding

De kwetsbaarheden betreffen onder andere:

- Een autorisatieprobleem waarbij geauthenticeerde gebruikers workflows kunnen toewijzen aan mappen binnen projecten waar zij geen toegang toe hebben, door onvoldoende validatie van request payloads tijdens workflow creatie.
- Een SQL-injectie in de legacy MySQL v1 node executeQuery operatie door onparameteriseerde expressie substitutie, wat het uitvoeren van willekeurige SQL statements toestaat.
- Verder kunnen geauthenticeerde gebruikers met de workflow:create permissie Object.prototype pollution veroorzaken via speciaal opgezette workflows, wat leidt tot ongeautoriseerde toegang tot privileged endpoints.
- Een andere kwetsbaarheid betreft het omzeilen van HTTP request domeinrestricties in de AI Agents functionaliteit door gebruikers met member-level permissies, wat kan resulteren in blootstelling van gedeelde credential secrets aan externe servers.
- Ook is er een probleem met onjuiste validatie van meerdere trusted token-exchange issuers, waardoor impersonatie van gebruikers over verschillende token issuers mogelijk is.
- Ten slotte kunnen gebruikers met editor toegang via HTTP Request node pagination expressies gevoelige credential data exfiltreren.

Deze kwetsbaarheden zijn aanwezig in verschillende versies van n8n en hebben betrekking op autorisatie, authenticatie, data-integriteit en vertrouwelijkheid binnen het platform.

Oplossingen

n8n heeft updates uitgebracht in versies 1.123.61, 2.27.4 en 2.28.1 om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/n8n-io/n8n/security/advisories/GHSA-2434-3x6q-8r99
- https://github.com/n8n-io/n8n/security/advisories/GHSA-2xgm-wc4g-5jvg
- https://github.com/n8n-io/n8n/security/advisories/GHSA-75qm-gp28-rcq9
- https://github.com/n8n-io/n8n/security/advisories/GHSA-h44j-f5r5-ph73
- https://github.com/n8n-io/n8n/security/advisories/GHSA-hwmj-qg4v-cvg9
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jp7m-xcgx-57qm
- https://github.com/n8n-io/n8n/security/advisories/GHSA-mq3m-f8x3-579w

- https://github.com/n8n-io/n8n/security/advisories/GHSA-q3j5-8vrg-4p9q
- https://github.com/n8n-io/n8n/security/advisories/GHSA-w867-jm58-p9pv

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-59253	5.3 MEDIUM
CVE-2026-59257	6.9 MEDIUM
CVE-2026-59206	7.1 HIGH
CVE-2026-59207	7.1 HIGH
CVE-2026-59208	7.6 HIGH
CVE-2026-59209	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-287	Improper Authentication
CWE-346	Origin Validation Error
CWE-522	Insufficiently Protected Credentials
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-693	Protection Mechanism Failure
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Getroffen producten

n8n
n8n

Disclaimer