Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0212

Kwetsbaarheden verholpen in n8n workflow automation platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 29-06-2026

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, specifiek in versies voor 1.123.55, 2.24.0, 2.25.7, 2.26.1 en 2.26.2.

Duiding

De kwetsbaarheden bereffen verschillende onderdelen van het n8n platform. Geuthenticeerde gebruikers met workflow bewerkingsrechten kunnen onder andere Content-Security-Policy (CSP) omzeilen via de Respond to Webhook node, en JavaScript injecteren via de Chat Trigger node. Verder kunnen zij API-tokens exfiltreren via de SecurityScorecard node en credentials van andere gebruikers benaderen, overschrijven of intrekken via de Dynamic Credentials feature. Ook kunnen gebruikers met editor toegang tot gedeelde workflows credentials van anderen inzien door onvoldoende eigendomcontroles.

Ongeauthenticeerde aanvallers kunnen via de MicrosoftAgent365Trigger en StripeTrigger nodes valse payloads indienen, wat leidt tot uitvoering van workflows met kwaadaardige data.

Oplossingen

n8n heeft updates uitgebracht in versies 1.123.55, 2.24.0, 2.25.7, 2.26.1 en 2.26.2 om de genoemde kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/n8n-io/n8n/security/advisories/GHSA-2j5h-858j-5mpf
- https://github.com/n8n-io/n8n/security/advisories/GHSA-2vff-hj5x-8gq7
- https://github.com/n8n-io/n8n/security/advisories/GHSA-42h7-m79w-wvg5
- https://github.com/n8n-io/n8n/security/advisories/GHSA-664h-gpgq-h6xx
- https://github.com/n8n-io/n8n/security/advisories/GHSA-9c38-2mcm-q7f7
- https://github.com/n8n-io/n8n/security/advisories/GHSA-c37g-w77q-m4vp
- https://github.com/n8n-io/n8n/security/advisories/GHSA-h3jj-5f3v-3685
- https://github.com/n8n-io/n8n/security/advisories/GHSA-h86q-fx34-gfjr
- https://github.com/n8n-io/n8n/security/advisories/GHSA-hv7x-3x78-gx53
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jpq7-226w-6cxx
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jqpw-qww5-cj4c
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jvc7-762p-3743
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jwm3-qcfw-c5pp
- https://github.com/n8n-io/n8n/security/advisories/GHSA-pmqw-72cg-wx85
- https://github.com/n8n-io/n8n/security/advisories/GHSA-qrx8-25qr-5r7v
- https://github.com/n8n-io/n8n/security/advisories/GHSA-rm2v-h48j-895m

- https://github.com/n8n-io/n8n/security/advisories/GHSA-v733-mwr6-fgcm
- https://github.com/n8n-io/n8n/security/advisories/GHSA-x6p3-m6h9-fx7r

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-54301	7.0 HIGH
CVE-2026-54302	7.0 HIGH
CVE-2026-54304	7.1 HIGH
CVE-2026-54305	8.9 HIGH
CVE-2026-54306	6.3 MEDIUM
CVE-2026-54307	8.5 HIGH
CVE-2026-54308	6.3 MEDIUM
CVE-2026-54309	8.8 HIGH
CVE-2026-54310	6.5 MEDIUM
CVE-2026-54311	6.0 MEDIUM
CVE-2026-54312	7.2 HIGH
CVE-2026-54313	6.5 MEDIUM
CVE-2026-54314	6.3 MEDIUM
CVE-2026-54303	6.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

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-284	Improper Access Control
CWE-290	Authentication Bypass by Spoofing
CWE-306	Missing Authentication for Critical Function
CWE-409	Improper Handling of Highly Compressed Data (Data Amplification)
CWE-488	Exposure of Data Element to Wrong Session
CWE-863	Incorrect Authorization
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Getroffen producten

n8n
n8n

Disclaimer