Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0248

## Kwetsbaarheden verholpen in n8n workflow automation platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2026

**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, specifiek in versies voor 2.10.1, 2.9.3, 1.123.22 en andere gerelateerde releases.

## Duiding

De kwetsbaarheden betreffen verschillende componenten binnen n8n, waaronder de Form nodes, Python Code node, JavaScript Task Runner sandbox, Merge node, Read/Write Files from Disk node, workflow expression evaluatie, core workflow editing functionaliteit, GitHub Webhook Trigger node, ZendeskTrigger node, Guardrail node en Chat Trigger node.

- Ongeauthenticeerde en geauthenticeerde gebruikers kunnen onder bepaalde voorwaarden arbitrary code injecteren en uitvoeren, soms via sandbox escapes, wat leidt tot remote code execution op het host-systeem.
- Kwetsbaarheden in nodes zoals Merge node en Read/Write Files from Disk node stellen geauthenticeerde gebruikers met workflow bewerkingsrechten in staat om bestanden te schrijven en shell-commando's uit te voeren.
- Webhook nodes (GitHub en ZendeskTrigger) missen HMAC-SHA256 handtekening verificatie, waardoor onbevoegde POST-requests kunnen worden verzonden die workflows triggeren.
- Authenticatie bypass kwetsbaarheden in SSO en Chat Trigger nodes maken het mogelijk om beveiligingsmechanismen te omzeilen en ongeautoriseerde toegang te verkrijgen.
- Input validatie in de Guardrail node kan worden omzeild, wat de integriteit van workflows kan aantasten.

Deze kwetsbaarheden zijn aanwezig in meerdere versies en releases van n8n en zijn gerelateerd aan workflow creatie, modificatie en uitvoering, waarbij misbruik kan leiden tot het overnemen van het host-systeem, het manipuleren van workflows en het omzeilen van authenticatiecontroles.

## Oplossingen

n8n heeft updates uitgebracht in versies 2.10.1, 2.9.3, 1.123.22, 2.8.0, 1.123.15, 2.5.0, 1.123.18, 2.6.2 en 2.10.0 om de genoemde kwetsbaarheden te verhelpen. Voor omgevingen waar directe upgrade niet mogelijk is, zijn tijdelijke mitigaties beschikbaar, zoals het beperken van gebruikersrechten en het uitschakelen van bepaalde nodes. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- https://github.com/n8n-io/n8n/security/advisories/GHSA-2p9h-rqjw-gm92
- https://github.com/n8n-io/n8n/security/advisories/GHSA-38c7-23hj-2wgq
- https://github.com/n8n-io/n8n/security/advisories/GHSA-75g8-rv7v-32f7
- https://github.com/n8n-io/n8n/security/advisories/GHSA-f3f2-mcxc-pwjx

- https://github.com/n8n-io/n8n/security/advisories/GHSA-fvfv-ppw4-7h2w
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jh8h-6c9q-7gmw
- https://github.com/n8n-io/n8n/security/advisories/GHSA-jjpj-p2wh-qf23
- https://github.com/n8n-io/n8n/security/advisories/GHSA-mmgg-m5j7-f83h
- https://github.com/n8n-io/n8n/security/advisories/GHSA-mqpr-49jj-32rc
- https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp
- https://github.com/n8n-io/n8n/security/advisories/GHSA-vjf3-2gpj-233v
- https://github.com/n8n-io/n8n/security/advisories/GHSA-vpcf-gvg4-6qwr
- https://github.com/n8n-io/n8n/security/advisories/GHSA-wxx7-mcgf-j869
- https://github.com/n8n-io/n8n/security/advisories/GHSA-x2mw-7j39-93xq

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2026-27493 | 9.5 CRITICAL |
| CVE-2026-27494 | 7.1 HIGH |
| CVE-2026-27495 | 9.4 CRITICAL |
| CVE-2026-27497 | 9.4 CRITICAL |
| CVE-2026-27498 | 9.0 CRITICAL |
| CVE-2026-27577 | 9.4 CRITICAL |
| CVE-2026-27578 | 8.5 HIGH |
| CVE-2026-56357 | 6.3 MEDIUM |
| CVE-2026-56350 | 6.0 MEDIUM |
| CVE-2026-56360 | 6.9 MEDIUM |
| CVE-2026-56349 | 6.3 MEDIUM |
| CVE-2026-56353 | 6.3 MEDIUM |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-20 | Improper Input Validation |
| 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-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| CWE-94 | Improper Control of Generation of Code ('Code Injection') |
| CWE-95 | Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') |
| CWE-269 | Improper Privilege Management |
| CWE-284 | Improper Access Control |
| CWE-285 | Improper Authorization |
| CWE-287 | Improper Authentication |
| CWE-290 | Authentication Bypass by Spoofing |
| CWE-345 | Insufficient Verification of Data Authenticity |
| CWE-497 | Exposure of Sensitive System Information to an Unauthorized Control Sphere |
| CWE-693 | Protection Mechanism Failure |
| CWE-913 | Improper Control of Dynamically-Managed Code Resources |
| CWE-937 | OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities |
| CWE-1035 | OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities |

## Getroffen producten

| **n8n** |
| --- |
| n8n |

## Disclaimer