مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Command Execution Vulnerability in n8n

Tracking #:432318358

Date:06-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Remote Command Execution security vulnerability has been identified in the n8n workflow automation platform.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in the n8n workflow automation platform, tracked as CVE-2026-25049 with a CVSS score of 9.4 (Critical).The flaw allows an authenticated user with workflow creation or modification privileges to execute arbitrary system commands on the underlying server by abusing crafted expressions inside workflows. This vulnerability is a bypass of protections introduced for the earlier critical issue CVE-2025-68613. When combined with n8n's public webhook feature, attackers can expose malicious workflows to the internet, enabling remote code execution (RCE) by unauthenticated external users.

Vulnerability Overview

- CVE ID: CVE-2026-25049
- CVSS Score: 9.4 (Critical)
- GHSA: GHSA-6cqr-8cfr-67f8
- Affected Product
- n8n Workflow Automation Platform

Affected Versions

- n8n < 1.123.17
- n8n < 2.5.2

Fixed Versions

- 1.123.17
- 2.5.2

Temporary Mitigations (If patching is not immediately possible)

These are short-term measures only and do NOT eliminate risk.

- Restrict workflow creation and editing to fully trusted users only
- Disable or tightly control public webhooks
- Deploy n8n in a hardened environment:
  - Run with minimal OS privileges
  - Apply strict network segmentation
  - Block outbound traffic where possible
- Monitor for:
  - Unexpected workflow changes
  - Suspicious webhook activity
  - Abnormal system commands or processes

RECOMMENDATIONS:

- Upgrade n8n immediately to one of the fixed version or latest version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/n8n-io/n8n/security/advisories/GHSA-6cqr-8cfr-67f8