Date Posted: 2026/03/03

[Vulnerability Alert] 4 Critical Security Vulnerabilities Found in n8n

- Subject Explanation: [Vulnerability Alert] 4 Critical Security Vulnerabilities Found in n8n

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000016
  - n8n is an open-source workflow automation tool that connects various applications via a visual drag-and-drop interface, allowing the automation of repetitive tasks without coding. Recently, n8n released a critical security advisory.
  - [CVE-2026-27495, CVSS: 9.4] This vulnerability allows an authenticated attacker with permissions to own or modify workflows to exploit a vulnerability in the JavaScript task execution sandbox, executing arbitrary code outside of its boundaries.
  - [CVE-2026-27493, CVSS: 9.5] This is a two-stage expression injection vulnerability. An unauthenticated attacker can inject and execute arbitrary n8n expressions via carefully crafted form data. If combined with the expression sandbox escape mechanism, it could lead to remote code execution on the n8n host.
  - [CVE-2026-27577, CVSS: 9.4] This vulnerability allows an authenticated attacker with permissions to create or modify workflows to use crafted workflow parameter expressions to trigger unauthorized system commands on the host executing n8n.
  - [CVE-2026-27498, CVSS: 9.0] This vulnerability allows an authenticated attacker with permissions to create or modify workflows to use git operations linked to the “Read/Write Files from Disk” node, leading to remote code execution.
- Impacted Platforms:
  - [CVE-2026-27495, CVE-2026-27493, CVE-2026-27577] n8n versions prior to 1.123.22, n8n versions from 2.0.0 prior to 2.9.3, n8n versions from 2.10.0 prior to 2.10.1
  - [CVE-2026-27498] n8n versions prior to 1.123.8, n8n versions prior to 2.2.0
- Suggested Measures:
  - [CVE-2026-27495, CVE-2026-27493, CVE-2026-27577] Please update to the following versions: n8n 1.123.22 and later versions, n8n 2.9.3 and later versions, n8n 2.10.1 and later versions
  - [CVE-2026-27498] Please update to the following versions: n8n 1.123.8 and later versions, n8n 2.2.0 and later versions
- * References:
  1. https://www.twcert.org.tw/tw/cp-169-10739-e7e58-1.html

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260303_24

Last update: **2026/03/03 15:36**