Date Posted: 2026/02/06

[Vulnerability Alert] Critical Security Vulnerability Found in n8n (CVE-2026-1470)

- Subject Explanation: [Vulnerability Alert] Critical Security Vulnerability Found in n8n (CVE-2026-1470)
- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202601-00000030
  - 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.
  - A critical security vulnerability advisory (CVE-2026-1470, CVSS: 9.9) was recently released. This is a remote code execution vulnerability that allows authenticated attackers to execute arbitrary code with the privileges of the n8n process, potentially leading to unauthorized access to sensitive data, tampering with workflows, and execution of system-level operations.
- Impacted Platforms:
  - n8n versions prior to 1.123.17
  - n8n versions from 2.0.0 to prior to 2.4.5
  - n8n versions from 2.5.0 to prior to 2.5.1
- Suggested Measures:
  - Please update to the following versions: n8n 1.123.17 or later, n8n 2.4.5 or later, n8n 2.5.1 or later
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10693-2b4a1-1.html

Computer and Communication Center Network Systems Division