Date Posted: 2026/02/10

[Vulnerability Alert] Critical Security Vulnerability Found in n8n (CVE-2026-25049)

- Subject Explanation: [Vulnerability Alert] Critical Security Vulnerability Found in n8n (CVE-2026-25049)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000004
  - 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 4.x: 9.4) was recently released. This vulnerability allows authenticated attackers with permissions to create or modify workflows to use crafted workflow parameter expressions to trigger unauthorized system commands on the host executing n8n.
- Impacted Platforms:
  - n8n versions prior to 1.123.17
  - n8n versions prior to 2.5.2
- Suggested Measures:
  - Please update to the following versions:
  - n8n 1.123.17 or later, n8n 2.5.2 or later
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10696-c7fdb-1.html

Computer and Communication Center
Network Systems Division