POSTING DATE: 2026/01/16

[VULNERABILITY ALERT] n8n Contains 4 Critical Security Vulnerabilities (CVE-2025-68613)(CVE-2025-68668)(CVE-2026-21877)(CVE-2026-21858)

- Subject: [VULNERABILITY ALERT] n8n Contains 4 Critical Security Vulnerabilities (CVE-2025-68613)(CVE-2025-68668)(CVE-2026-21877)(CVE-2026-21858)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202601-00000014
  - n8n is an open-source workflow automation tool that connects multiple applications through a visual drag-and-drop interface, automating repetitive tasks without the need for code. Recently, n8n released several critical security vulnerability announcements.
  - [CVE-2025-68613, CVSS: 9.9] This is a remote code execution vulnerability that, under specific conditions, allows an authenticated attacker to execute arbitrary code with the permissions of the n8n process.
  - [CVE-2025-68668, CVSS: 9.9] Due to a sandbox bypass vulnerability in the Python code node using Pyodide in n8n, an authenticated attacker with permissions to create or modify workflows can execute arbitrary commands on the n8n server with the same permissions as the n8n process.
  - [CVE-2026-21877, CVSS: 10.0] This vulnerability allows an authenticated attacker to exploit n8n services to execute malicious code, leading to a complete compromise of the system.
  - [CVE-2026-21858, CVSS: 10.0] This vulnerability allows an unauthenticated attacker to access files on the underlying server through the execution of certain form-based workflows, resulting in the leakage of sensitive data stored in the system.
- Affected Platforms:
  - n8n versions 0.211.0 to 1.120.4 (exclusive)
  - n8n version 1.121.0
  - n8n versions 1.0.0 to 2.0.0 (exclusive)
  - n8n version 0.121.2 (inclusive) and earlier
  - n8n versions 1.65.0 to 1.121.0 (exclusive)
- Recommended Actions:
  - [CVE-2025-68613] Please update to the following versions: n8n version 1.120.4, version 1.121.1, or version 1.122.0
  - [CVE-2025-68668] Please update to the following version: n8n version 2.0.0
  - [CVE-2026-21877] Please update to the following version: n8n version 1.121.3
  - [CVE-2026-21858] Please update to the following version: n8n version 1.121.0
- Reference Material:
  1. https://www.twcert.org.tw/tw/cp-169-10636-1fa36-1.html

Computer and Communication Center
Network Systems Division, Respectfully