مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in n8n
Tracking #:432318214
Date:06-01-2026

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in n8n that could be exploited to execute arbitrary operating system commands on the underlying host, potentially leading to full system compromise.

TECHNICAL DETAILS:

A critical security vulnerability has been disclosed in **n8n**, an open-source workflow automation platform. The flaw could allow an authenticated attacker to execute arbitrary operating system commands on the underlying host, potentially leading to full system compromise.

Vulnerability Details
- **CVE-2025-68668**
- **CVSS Score:** 9.9 (Critical)
- **Vulnerability Type:** Protection Mechanism Failure / Sandbox Bypass
- The vulnerability exists within the Python Code Node that uses Pyodide. An authenticated user with permission to create or modify workflows can bypass sandbox restrictions and execute arbitrary system commands on the host running n8n, inheriting the same privileges as the n8n process.
- Successful exploitation could allow attackers to:
    - Execute arbitrary commands on the host system
    - Compromise the integrity and confidentiality of the underlying server
    - Escalate attacks to other systems connected to the affected environment
- **Affected Versions:** n8n versions 1.0.0 up to, but not including, 2.0.0
- **Fixed Version:** n8n 2.0.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by n8n.

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://nvd.nist.gov/vuln/detail/CVE-2025-68668