مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in n8n

Tracking #:432318166

Date:23-12-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical Remote Code Execution (RCE) vulnerability has been disclosed in the n8n workflow automation platform.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) vulnerability, tracked as CVE-2025-68613 with a CVSS score of 9.9/10, has been disclosed in the n8n workflow automation platform. The flaw allows authenticated attackers to execute arbitrary operating system commands on the underlying server through expression injection in workflow definitions.
Exploitation can result in full server compromise, including unauthorized access to sensitive data, manipulation or destruction of workflows, and potential lateral movement across connected infrastructure.

Vulnerability Details:

- CVE ID: CVE-2025-68613
- Severity: Critical
- CVSS Score: 9.9 / 10
- Vulnerability Type: Remote Code Execution (RCE)
- Attack Vector: Authenticated
- Privileges Required: Low (workflow creation or editing)
- User Interaction: Required
- Impact: Full system compromise

Affected Version:

- n8n (npm) >= 0.211.0 < 1.120.4

Fixed Version:

- 1.120.4, 1.121.1, 1.122.0.

RECOMMENDATIONS:

- Upgrade Immediately-Update n8n to one of the mentioned fixed versions.

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://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp