Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

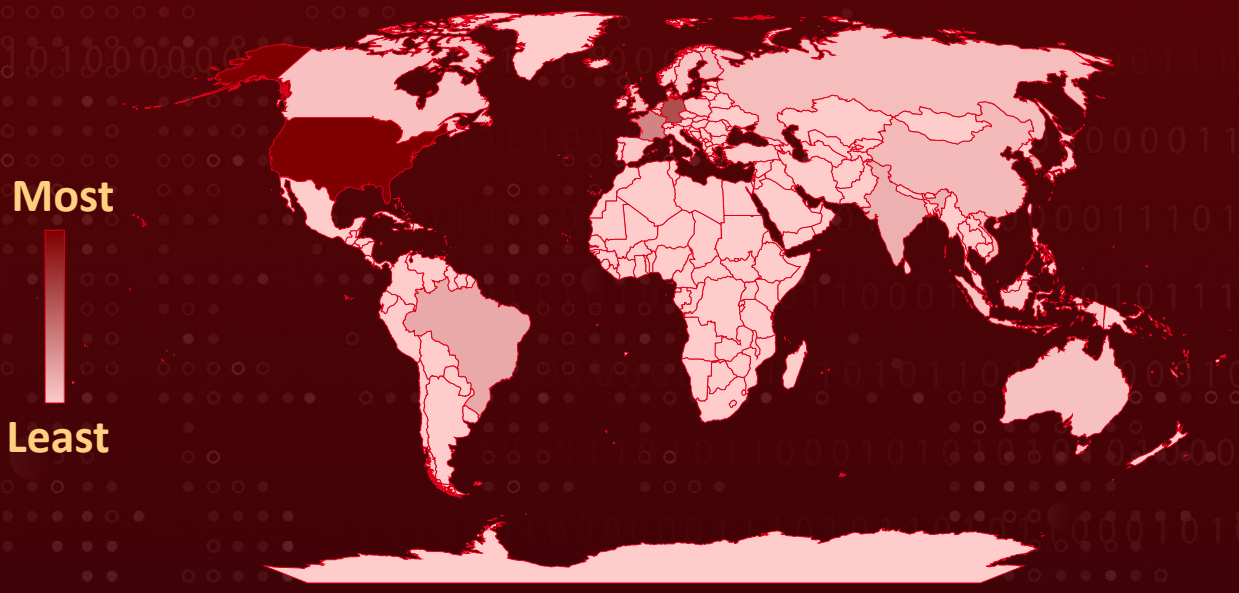
# Automation Gone Rogue: CVE-2025-68613 Puts n8n Instances at Risk


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| December 24, 2025 | A1 | TA2025388 |

# Summary

**First Seen:** December 19, 2025
**Affected Product:** n8n
**Impact:** CVE-2025-68613 is a critical remote code execution vulnerability in the n8n workflow automation platform caused by insufficient sandbox isolation in its expression evaluation engine. Authenticated attackers with workflow editing privileges can inject malicious expressions that escape the execution context and run arbitrary operating system commands with n8n process privileges, leading to full instance compromise, data exposure, and workflow manipulation.

## Targeted Regions




## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2025-68613 | n8n Remote Code Execution via Expression Injection Vulnerability | n8n | ✗ | ✗ | ✓ |

# Vulnerability Details

**#1**

A critical security flaw has been disclosed in the n8n workflow automation platform that enables remote code execution under specific conditions. Tracked as CVE-2025-68613, the vulnerability affects a widely adopted package with approximately 57,000 weekly downloads, amplifying its operational risk.

**#2**

The issue originates in n8n's workflow expression evaluation engine. When authenticated users create or modify workflows, they can embed expressions that are executed by the runtime. Due to inadequate sandbox isolation, these expressions are not sufficiently contained. As a result, crafted inputs can escape their intended execution boundaries and interact directly with the system-level operations.

**#3**

This weakness constitutes a critical Remote Code Execution vulnerability caused by improper control over dynamically managed code resources. The platform fails to adequately restrict access to variables, objects, classes, functions, and executable instructions during expression evaluation. An attacker with workflow editing privileges can exploit this gap by injecting malicious expressions into a workflow configuration.

**#4**

Once processed, the malicious expressions break out of the evaluation context and execute arbitrary operating system commands with the same privileges as the n8n process. Successful exploitation can lead to complete compromise of the affected instance, including unauthorized access to sensitive data, manipulation of workflows, execution of system-level operations, and potential lateral movement within the environment.

**#5**

The vulnerability impacts n8n deployments across a broad range of scenarios, including self-hosted enterprise installations, internet-facing cloud deployments, multi-tenant automation environments, embedded automation use cases, and CI/CD pipelines that rely on n8n for orchestration. *Exposed instances are most heavily concentrated in the United States, followed by Germany, France, Brazil, and Singapore.* Given the potential for full instance takeover and widespread operational impact, CVE-2025-68613 represents a high-severity risk that demands immediate remediation.

# Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2025-68613 | n8n all versions starting with 0.211.0 and prior to 1.120.4 | cpe:2.3:a:n8n:n8n:*:*:*:*:*:*:node.js:*:* | CWE-913 |

# Recommendations

**Immediate Upgrade to Patched Version:** Upgrade n8n to version 1.120.4, 1.121.1, 1.122.0 or later without delay. This release fixes CVE-2025-68613 by strengthening sandbox isolation and enforcing stricter controls on expression evaluation, effectively closing the remote code execution vector. Patch first in cloud-hosted, multi-tenant, CI/CD, and internet-accessible instances where attackers reach, and impact is highest.

**Restrict Workflow Permissions:** Limit workflow creation and editing rights to a minimal set of fully trusted users. Since exploitation requires authenticated access with workflow modification privileges, reducing this surface directly lowers risk.

**Harden the Execution Environment:** Run n8n with the least possible operating system privileges and apply strict filesystem, process, and network restrictions. This constrains attacker capabilities even if expression escape is attempted.

**Audit and Monitor Workflows:** Review existing workflows for suspicious expressions and monitor execution behavior for anomalies. Post-exploitation detection is essential for environments that have delayed upgrading.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Execution | T1059: Command and Scripting Interpreter | |
| | T1203: Exploitation for Client Execution | |
| Privilege Escalation | T1068: Exploitation for Privilege Escalation | |
| Defense Evasion | T1211: Exploitation for Defense Evasion | |
| Persistence | T1546: Event Triggered Execution | |
| Collection | T1005: Data from Local System | |
| Impact | T1565: Data Manipulation | T1565.001: Stored Data Manipulation |

## Patch Link

https://github.com/n8n-io/n8n/releases

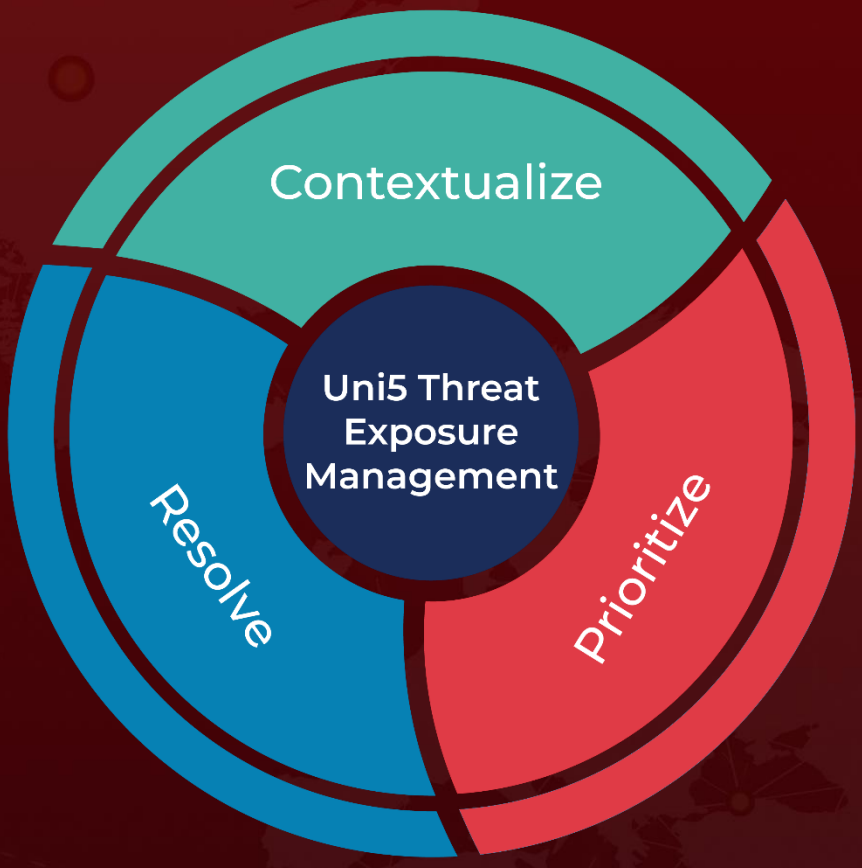
## Reference

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

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**December 24, 2025 • 08:30 AM**



More at www.hivepro.com