Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ni8mare in n8n: CVE-2026-21858 Bug Exposing 100,000 Servers to Risk

Date of Publication	Admiralty Code	TA Number
January 16, 2026	A1	TA2026016

Summary

First Seen: November 9, 2025
Affected Product: n8n
Impact: A critical vulnerability dubbed Ni8mare (CVE-2026-21858) has been discovered in n8n, a popular open-source workflow automation platform, allowing unauthenticated remote attackers to read arbitrary server files and escalate to code execution. Because n8n often functions as a central automation hub with access to critical services such as cloud storage, databases, and CI/CD pipelines, a single compromised instance can cascade into a full infrastructure breach. Organizations face potential exposure of sensitive business data, credential theft enabling lateral movement, and complete infrastructure compromise, depending on deployment configuration and workflow usage patterns.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-21858	Ni8mare (n8n Unauthenticated Remote Code Execution Vulnerability)	n8n	✗	✗	✓

Vulnerability Details

#1

A maximum-severity vulnerability known as Ni8mare has been identified in n8n, a widely used open-source workflow automation platform. Tracked as CVE-2026-21858, the flaw allows unauthenticated remote attackers to read arbitrary files from the underlying server and ultimately take full control of affected instances. With over 100 million Docker pulls and an estimated 100,000 exposed servers, the impact is global and immediate.

#2

The vulnerability originates in form-based workflow handling. n8n fails to correctly validate request content types in its webhook processing logic. By manipulating the Content-Type header, an attacker can overwrite internal file references and force the platform to process attacker-supplied file paths. This enables direct access to sensitive server files, including the n8n database and configuration secrets. Once these are extracted, attackers can forge sessions, bypass authentication, and escalate the attack to remote code execution, resulting in complete server compromise.

#3

The risk extends far beyond a single system. n8n often acts as the central automation hub for organizations, storing OAuth tokens, API keys, database credentials, and cloud access for services such as Google Drive, Salesforce, payment platforms, internal databases, and CI/CD pipelines. A compromised instance exposes every connected system, enabling credential theft, lateral movement, and large-scale data breaches.

#4

While exploitation requires a publicly accessible form workflow and a method to retrieve stolen data, the consequences are severe. There are no effective workarounds. Organizations must upgrade to n8n version 1.121.0 or later immediately. Concurrently, related supply-chain attacks have emerged, including malicious community npm packages designed to harvest credentials from vulnerable n8n environments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-21858	n8n version 1.65.0 - 1.120.0	cpe:2.3:a:n8n:n8n:*:*:*:*:*:*:*:*	CWE-20

Recommendations

Upgrade to Patched Version Immediately: Install n8n version 1.121.0 or later without delay, as this patch directly addresses the Content-Type confusion vulnerability. Organizations running self-hosted Docker deployments should pull the latest image and redeploy, while those using npm-based installations should run npm update to obtain the patched version.

Restrict Network Exposure: Avoid exposing n8n instances directly to the internet unless necessary for business operations. Place n8n servers behind VPNs, reverse proxies with authentication, or network firewalls that limit access to trusted IP ranges. This reduces the attack surface by preventing unauthenticated external actors from reaching vulnerable form endpoints.

Enforce Authentication on All Form Endpoints: Configure all n8n forms to require authentication before accepting submissions. Review existing workflows and disable or remove any publicly accessible webhook and form endpoints that do not have a legitimate business requirement for unauthenticated access. This serves as a temporary mitigation measure for organizations unable to immediately patch.

Audit Community Node Installations: Review all installed community nodes (npm packages) in your n8n environment, particularly those added recently. Remove any packages with suspicious characteristics such as random names, empty descriptions, low download counts, or missing documentation. Prefer official n8n integrations over community-contributed nodes when possible, and audit source code before installing any third-party packages.

Rotate Credentials and API Keys: If exploitation cannot be ruled out, rotate all credentials stored in the n8n credential store, including OAuth tokens, API keys, database connection strings, and service account passwords. Change the n8n encryption secret key and regenerate all session tokens to invalidate any potentially forged authentication cookies.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Persistence	T1078: Valid Accounts	T1078.003: Local Accounts
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Collection	T1005: Data from Local System	
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Package Name	n8n-nodes-hfgjf-irtuinvcm-lasdqewriit
Domain	n8n-license-validator[.]onrender[.]com

TYPE	VALUE
SHA256	b435f95ad1dc9b1830798b2ed0dd2c891ef158dd7b622bd135c2214c26fe7998, f458ee2b1cf41e00de31e1bb727a876f6927ac61d53a502817180f6b8ebbb72b, 38931ec67a3ebdb344fd0a2c92865cc3cfb07e8e6d161c91ad36425c11fb0ef6

Patch Details

The issue has been fixed in n8n version 1.121.0. Users should upgrade to this version or later to remediate the vulnerability.

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

References

https://github.com/n8n-io/n8n/security/advisories/GHSA-v4pr-fm98-w9pg

https://www.cyera.com/research-labs/ni8mare-unauthenticated-remote-code-execution-in-n8n-cve-2026-21858

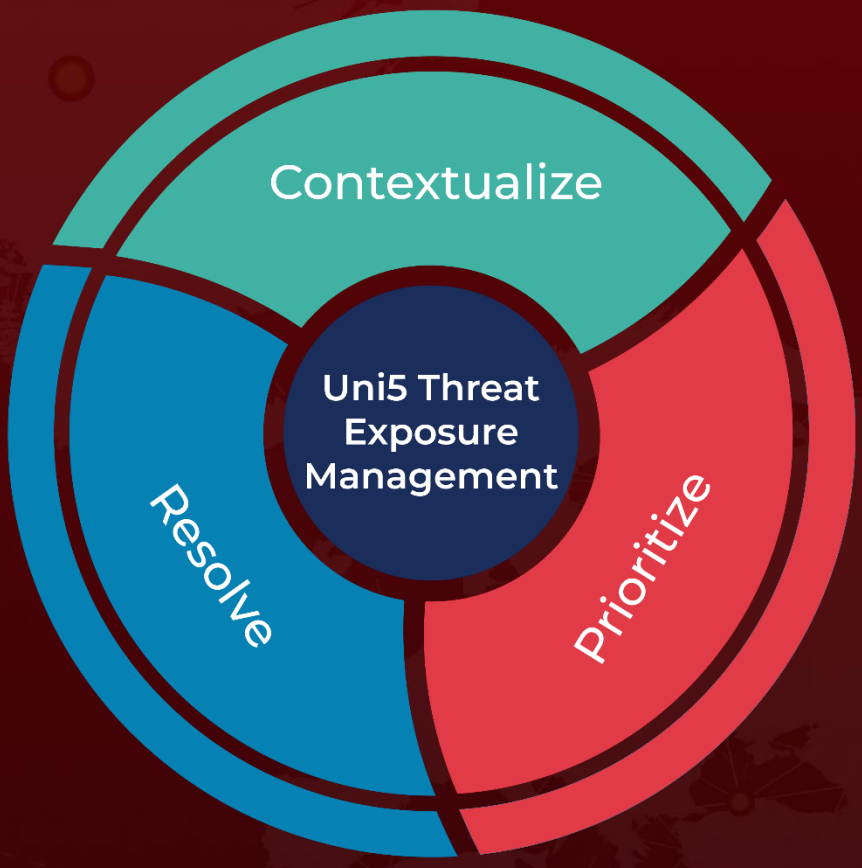
https://www.endorlabs.com/learn/n8mare-on-auth-street-supply-chain-attack-targets-n8n-ecosystem

https://hivepro.com/threat-advisory/automation-gone-rogue-cve-2025-68613-puts-n8n-instances-at-risk/

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

January 16, 2026 • 06:00 AM

More at www.hivepro.com