# Critical n8n Security Update: Public RCE Vulnerability PoC Now Available

*SecureLayer7 Blackf0g researcher team A critical RCE vulnerability in n8n has been identified and patched.*

AUSTIN, TX, UNITED STATES, February 4, 2026 /EINPresswire.com/ -- SecureLayer7 Research Labs has identified and responsibly disclosed a critical Remote Code Execution (RCE) vulnerability, CVE-2026-25049, affecting the n8n workflow automation platform.

> n8n's AI workflow platform is widely used by enterprises. CVE-2026-25049 shows why deep, assumption-driven security validation is no longer optional. AI led security research is redefining pentest"
>
> *Sandeep Kamble, CTO at SecureLayer7*

The vulnerability impacts n8n's expression evaluation and sandboxing logic, enabling attackers to bypass security controls and execute arbitrary commands on the underlying host system. Successful exploitation may result in full server compromise, credential exposure, workflow manipulation, and potential lateral movement.

The discovery was made using SecureLayer7's proprietary, non-public, fine-tuned AI security research model, developed specifically for advanced vulnerability discovery and sandbox bypass analysis. The model enables deep programmatic reasoning across modern automation frameworks and assisted researchers in identifying critical assumption failures within the platform's execution flow.

SecureLayer7 coordinated responsibly with the n8n security team, and the issue has been patched in the latest releases. Users are strongly advised to upgrade immediately to mitigate risk.

Organizations operating n8n instances should:
1. Upgrade to the latest secure version
2. Restrict public exposure of automation interfaces
3. Review logs for suspicious activity

This disclosure reinforces the need for assumption-driven security validation in dynamic execution environments and highlights the growing role of AI-assisted offensive research in identifying complex logic flaws.

For technical details and mitigation guidance, refer to the SecureLayer7 advisory:
https://blog.securelayer7.net/cve-2026-25049/?utm_source=chatgpt.com

About SecureLayer7
SecureLayer7 is a cybersecurity research and offensive security company specializing in advanced vulnerability discovery, red teaming, and AI-driven security testing solutions.

Sandeep Kamble
SecureLayer7 cybersecurity INC.
+1 737-342-3067
email us here
Visit us on social media:
LinkedIn
YouTube

---