



An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2602270221

NCSC Advisory

Critical Remote Code Execution Vulnerability in n8n n8n-io

CVE-2026-27497

27th, February 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-27497**Published:** 2026-02-25**Vendor:** n8n**Product:** n8n-io**CVSS Score¹:** 9.4

Products Affected

Product	Version
n8n	< 1.123.22
n8n	>= 2.0.0, < 2.9.3
n8n	>= 2.10.0, < 2.10.1

Impact

n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could leverage the Merge node's SQL query mode to execute arbitrary code and write arbitrary files on the n8n server.

The issues have been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate all known vulnerabilities. If upgrading is not immediately possible, administrators should consider the following temporary mitigations.

Limit workflow creation and editing permissions to fully trusted users only, and/or disable the Merge node by adding `n8n-nodes-base.merge` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.

¹ <https://www.first.org/cvss/>

TLP: CLEAR

Rialtas na hÉireann
Government of Ireland



Common Weakness Enumeration (CWE)²: CWE-94: Improper Control of Generation of Code ('Code Injection'), CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from n8n-io.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-27497>
- <https://www.cve.org/CVERecord?id=CVE-2026-27497>
- <https://community.n8n.io/t/security-bulletin-february-25-2026/270324>
- <https://github.com/n8n-io/n8n/security/advisories/GHSA-wxx7-mcgf-j869>
- <https://github.com/n8n-io/n8n/releases/tag/n8n@1.123.22>
- <https://github.com/n8n-io/n8n/releases/tag/n8n@2.10.1>
- <https://github.com/n8n-io/n8n/releases/tag/n8n@2.9.3>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>