XML Node Prototype Pollution to RCE

Critical **Jubke** published **GHSA-hqr4-h3xv-9m3r** 2 weeks ago

Package

n8n (npm)

Affected versions	Patched versions
< 2.18.1	>= 2.18.1
< 2.17.4	>= 2.17.4
< 1.123.32	>= 1.123.32

Description

Impact

An authenticated user with permission to create or modify workflows could achieve global prototype pollution via the XML Node leading to RCE when combined with other nodes exploiting the prototype pollution.

Patches

The issue has been fixed in n8n versions 1.123.32, 2.17.4, and 2.18.1. Users should upgrade to one of these versions or later to remediate the vulnerability.

Workarounds

If upgrading is not immediately possible, administrators should consider the following temporary mitigations:

- Limit workflow creation and editing permissions to fully trusted users only.
- Disable the XML node by adding `n8n-nodes-base.xml` to the `NODES_EXCLUDE` environment variable.

These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.

n8n has adopted CVSS 4.0 as primary score for all security advisories. CVSS 3.1 vector strings are provided for backwards compatibility.

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Severity

Critical 9.4 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	Low

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:L

CVE ID

CVE-2026-42232

Weaknesses

No CWEs

Credits

 **simonkoeck** Reporter