Prototype Pollution in XML Webhook Body Parser Leads to RCE

Critical **Jubke** published **GHSA-q5f4-99jv-pgg5** 2 weeks ago

Package

n8n (npm)

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

Description

Impact

A flaw in the `xml2js` library used to parse XML request bodies in n8n's webhook handler allowed prototype pollution via a crafted XML payload. An authenticated user with permission to create or modify workflows could exploit this to pollute the JavaScript object prototype and, by chaining the pollution with the Git node's SSH operations, achieve remote code execution on the n8n host.

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.

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:N/UI:N/S:C/C:H/I:H/A:H

Severity

Critical 10.0 / 10

CVSS v4 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-42231

Weaknesses

No CWEs

Credits

a-tallat Reporter