Python Task Runner Sandbox Escape

High **Jubke** published **GHSA-44v6-jhgm-p3m4** 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

An authenticated user with permission to create or modify workflows containing a Python Code Node could escape the sandbox and achieve arbitrary code execution on the task runner container.

- This issue only affects instances where the Python Task Runner is enabled.

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 Python Code node by adding `n8n-nodes-base.code` to the `NODES_EXCLUDE` environment variable, or disable the Python Task Runner entirely.

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:U/C:H/I:L/A:N

Severity

High 7.1 / 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	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-42234

Weaknesses

▶ CWE-94

Credits

dorjoos Reporter