Windmill Exposes Workspace Slack OAuth Client Secrets to Non-Admin Workspace Members

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-26964
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-20 00:16:16 UTC
Updated	2026-04-14 00:50:19 UTC
Description	Windmill is an open-source developer platform for internal code: APIs, background jobs, workflows and UIs. Versions 1.634

Risk And Classification

Primary CVSS: v3.1 2.7 LOW from security-advisories@github.com

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

Problem Types: CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Windmill	Windmill	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Windmill-labs	Windmill	affected < 1.635.0	Not specified

References

Reference	Source	Link	Tags
github.com/windmill-labs/windmill/security/advisories/GHSA-f27g-j463-q85w	security-advisories@github.com	github.com	Exploit, V
github.com/windmill-labs/windmill/releases/tag/v1.635.0	security-advisories@github.com	github.com	Product,
github.com/windmill-labs/windmill/commit/43218c62852490d0efafa8f94385bfe...	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.