Windmill < 1.603.3 File Ownership Handling SQLi RCE

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

Summary

CVE	CVE-2026-23696
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 17:16:27 UTC
Updated	2026-04-07 17:16:27 UTC
Description	Windmill CE and EE versions 1.276.0 through 1.603.2 contain an SQL injection vulnerability in the folder ownership manag

Risk And Classification

Primary CVSS: v4.0 9.4 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/S
4.0	CNA	CVSS	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/S
3.1	disclosure@vulncheck.com	Primary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Windmill Labs	Windmill CE Community Edition	affected 1.276.0 1.603.2 semver	Not specified
CNA	Windmill Labs	Windmill CE Community Edition	unaffected 1.603.3	Not specified
CNA	Windmill Labs	Windmill EE Enterprise Edition	affected 1.276.0 1.603.2 semver	Not specified
CNA	Windmill Labs	Windmill EE Enterprise Edition	unaffected 1.603.3	Not specified
CNA	Nextcloud	Flow	affected 1.0.0 1.2.2 semver	Not specified

CNA	Nextcloud	Flow	affected 1.0.0 1.2.2 semver	Not specified
CNA	Nextcloud	Flow	unaffected 1.3.0	Not specified
CNA	Nextcloud	Flow	unaffected 1.3.1	Not specified

References

Reference	Source	Link	Tags
github.com/Chocapikk/Windfall	disclosure@vulncheck.com	github.com	
github.com/windmill-labs/windmill/releases/tag/v1.603.3	disclosure@vulncheck.com	github.com	
www.windmill.dev	disclosure@vulncheck.com	www.windmill.dev	
apps.nextcloud.com/apps/flow/releases	disclosure@vulncheck.com	apps.nextcloud.com	
www.vulncheck.com/advisories/windmill-file-ownership-handling-sqli-rce	disclosure@vulncheck.com	www.vulncheck.com	
chocapikk.com/posts/2026/windfall-nextcloud-flow-windmill-rce	disclosure@vulncheck.com	chocapikk.com	
github.com/windmill-labs/windmill/commit/942fb629210ebb287f48467d1535ffd...	disclosure@vulncheck.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

Vendor Comments And Credit

Discovery Credit

CNA: Valentin Lobstein (Chocapikk) (en)

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