Focalboard Second-Order SQL Injection in category reorder endpoint allows data exfiltration (unsupported product, no fix)

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

Summary

CVE	CVE-2026-25773
State	PUBLISHED
Assigner	Mattermost
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 14:16:29 UTC
Updated	2026-04-28 00:19:15 UTC
Description	** UNSUPPORTED WHEN ASSIGNED ** Focalboard version 8.0 fails to sanitize category IDs before incorporating them in

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000100000 probability, percentile 0.010020000 (date 2026-04-07)

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
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	responsibledisclosure@mattermost.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mattermost	Focalboard	8.0.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mattermost	Focalboard	affected 8.0 semver	Not specified

References

Reference	Source	Link	Tags
github.com/mattermost-community/focalboard	responsibledisclosure@mattermost.com	github.com	Product
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Siam Thanat Hack Company Limited (pentest@sth.sh) (en)

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