Insufficient token rotation validation in remote cluster invite confirmation

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

Summary

CVE	CVE-2026-4273
State	PUBLISHED
Assigner	Mattermost
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-18 08:16:14 UTC
Updated	2026-05-18 17:32:38 UTC
Description	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to validate that the RefreshedToken differs from the original

Risk And Classification

Primary CVSS: v3.1 3.7 LOW from responsibledisclosure@mattermost.com

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

EPSS: 0.000280000 probability, percentile 0.080870000 (date 2026-05-18)

Problem Types: CWE-863 | CWE-863 CWE-863: Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	responsibledisclosure@mattermost.com	Secondary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mattermost	Mattermost	affected 11.5.0 11.5.1 semver	Not specified
CNA	Mattermost	Mattermost	affected 10.11.0 10.11.13 semver	Not specified
CNA	Mattermost	Mattermost	unaffected 11.6.0	Not specified
CNA	Mattermost	Mattermost	unaffected 11.5.2	Not specified
CNA	Mattermost	Mattermost	unaffected 10.11.14	Not specified

References

Reference	Source	Link	Tags
mattermost.com/security-updates	responsibledisclosure@mattermost.com	mattermost.com	
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: daw10 (en)

Additional Advisory Data

Solutions

CNA: Update Mattermost to versions 11.6.0, 11.5.2, 10.11.14 or higher.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**