



OAuth authorization code client binding not enforced during token redemption in Mattermost

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-6334
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 08:16:14 UTC
Description	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to enforce client identity binding during the OAuth authorizat

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from responsiblydisclosure@mattermost.com

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

Problem Types: CWE-305 | CWE-305 CWE-305 – Authentication Bypass by Primary Weakness

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/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: Dylan Haussermann (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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

