



# CSRF Protection Bypass Allows Updating a User's Authentication Method

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

## Summary

<b>CVE</b>	CVE-2026-28741
<b>State</b>	PUBLISHED
<b>Assigner</b>	Mattermost
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 11:16:33 UTC
<b>Updated</b>	2026-04-22 19:42:25 UTC
<b>Description</b>	Mattermost versions 10.11.x <= 10.11.12, 11.5.x <= 11.5.0, 11.4.x <= 11.4.2, 11.3.x <= 11.3.2 fail to validate CSRF tokens

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from nvd@nist.gov

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

**EPSS:** 0.000160000 probability, percentile 0.035320000 (date 2026-04-21)

**Problem Types:** CWE-352 | CWE-352 CWE-352: Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	responsibledisclosure@mattermost.com	Secondary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mattermost	Mattermost Server	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mattermost	Mattermost	affected 10.11.0 10.11.12 semver	Not specified
CNA	Mattermost	Mattermost	affected 11.5.0 11.5.0 semver	Not specified
CNA	Mattermost	Mattermost	affected 11.4.0 11.4.2 semver	Not specified
CNA	Mattermost	Mattermost	affected 11.3.0 11.3.2 semver	Not specified
CNA	Mattermost	Mattermost	unaffected 10.11.13	Not specified
CNA	Mattermost	Mattermost	unaffected 11.5.1	Not specified
CNA	Mattermost	Mattermost	unaffected 11.4.3	Not specified
CNA	Mattermost	Mattermost	unaffected 11.3.3	Not specified

### References

Reference	Source	Link	Tags
mattermost.com/security-updates	responsibledisclosure@mattermost.com	mattermost.com	Vendor Advisory
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:** Eva Sarafianou (en)

### Additional Advisory Data

Solutions

**CNA:** Update Mattermost to versions 10.11.13, 11.5.1, 11.4.3, 11.3.3 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)