



Unbounded Request Body Read in MS Teams Plugin `changes` Webhook Endpoint

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

Summary

CVE	CVE-2026-24661
State	PUBLISHED
Assigner	Mattermost
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 11:16:21 UTC
Updated	2026-04-17 20:31:03 UTC
Description	Mattermost Plugins versions <=2.1.3.0 fail to limit the request body size on the <code>changes</code> webhook endpoint which allows

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:N/I:N/A:H](#)

EPSS: 0.000510000 probability, percentile 0.157100000 (date 2026-04-17)

Problem Types: CWE-770 | CWE-770 CWE-770: Allocation of Resources Without Limits or Throttling

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:N/I:N/A:H
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:N/A:L
3.1	CNA	CVSS	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mattermost	Mattermost	affected 2.1.3 semver	Not specified
CNA	Mattermost	Mattermost	unaffected 2.3.2.0	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: [Lorenzo Gallegos \(en\)](#)

Additional Advisory Data

Solutions

CNA: Update Mattermost Plugins to versions 2.3.2.0 or higher.

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

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