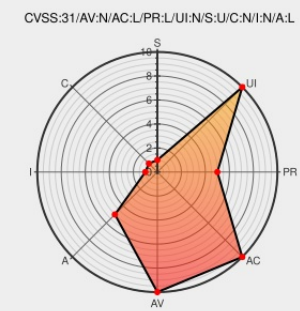
CVE-2022-2406

Published on: Not Yet Published

Last Modified on: 06/30/2023 06:49:00 PM UTC

CVE-2022-2406 - advisory for MMSA-2022-00102

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mattermost from Mattermost contain the following vulnerability:

The legacy Slack import feature in Mattermost version 6.7.0 and earlier fails to properly limit the sizes of imported files, which allows an authenticated attacker to crash the server by importing large files via the Slack import REST API.

CVE-2022-2406 has been assigned by responsibledisclosure@mattermost.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Mattermost** - **Mattermost** version **<= 6.3.8**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **= 6.4.x**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **<= 6.5.1**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **<= 6.6.1**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **= 6.7.0**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Security Updates - Mattermost Open Source Collaboration Platform	mattermost.com text/html	MISC mattermost.com/security-updates/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mattermost	Mattermost	6.6.0	All	All	All
Application	Mattermost	Mattermost	6.6.1	All	All	All
Application	Mattermost	Mattermost	6.7.0	All	All	All
Application	Mattermost	Mattermost	All	All	All	All
Application	Mattermost	Mattermost	All	All	All	All

cpe:2.3:a:mattermost:mattermost:6.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:mattermost:mattermost:6.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mattermost:mattermost:6.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:mattermost:mattermost:*:*:*:*:*:*:*:*:

cpe:2.3:a:mattermost:mattermost:*:*:*:*:*:*:*:*:

Discovery Credit

Thanks to Juho Nurminen for contributing to this improvement under the Mattermost responsible disclosure policy.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-2406 : The legacy Slack import feature in Mattermost version 6.7.0 and earlier fails to properly limit the… twitter.com/i/web/status/1…	2022-07-14 18:08:11
/r/netcve	CVE-2022-2406	2022-07-14 18:38:47

← Previous ID Next ID→