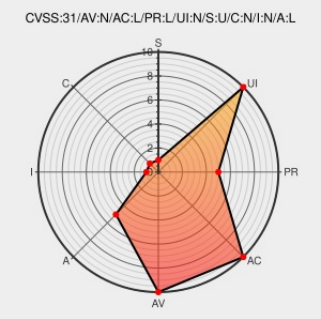
CVE-2022-1337

Published on: Not Yet Published

Last Modified on: 07/21/2023 04:55:00 PM UTC

CVE-2022-1337 - advisory for MMSA-2022-0090

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



Certain versions of Mattermost Server from Mattermost contain the following vulnerability:

The image proxy component in Mattermost version 6.4.1 and earlier allocates memory for multiple copies of a proxied image, which allows an authenticated attacker to crash the server via links to very large image files.

CVE-2022-1337 has been assigned by responsibledisclosure@mattermost.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Mattermost** - **Mattermost** version **< 6.4.2**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **< 6.3.5**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **< 6.2.5**

Affected Vendor/Software: **Mattermost** - **Mattermost** version **< 5.37.9**

Vulnerability Patch/Work Around

Disable the image proxy or use an external proxy.

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/

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 Server	All	All	All	All

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

Discovery Credit

Thanks to Agniva de Sarker for contributing to this improvement under the Mattermost responsible disclosure policy.

Social Mentions

Source	Title	Posted (UTC)
@ICS_Mikko	@ICS_SCADA CVE-2022-1337: Critical Bugs Allow Code Execution and Environmental Impact on WirelessFART. Discovered by Joseph Pujol.	2022-01-29 06:07:07
/r/RedSec	Happy Cakeday, r/RedSec! Today you're 10	2022-10-11 06:32:10

← Previous ID

Next ID→