Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0068

Kwetsbaarheden verholpen in Mattermost

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-02-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Mattermost heeft kwetsbaarheden verholpen in versies 10.4.x, 9.11.x, 10.3.x, 10.2.x en 10.1.x.

Duiding

De kwetsbaarheden omvatten onder andere het niet ongeldig maken van actieve sessies bij conversie naar een bot, onjuiste invoervalidatie tijdens het patchen en dupliceren van borden, SQL-injectie-aanvallen door het ontbreken van voorbereide statements in SQL-query's, onjuiste exportrestricties van archiefkanalen en onjuiste validatie van bordblokken bij het importeren van speciaal vervaardigde archieven. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang tot gevoelige informatie en mogelijk uitvoer van willekeurige code.

Oplossingen

Mattermost heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://mattermost.com/security-updates

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-1412	6.3 MEDIUM
CVE-2025-20051	5.3 MEDIUM
CVE-2025-24490	5.3 MEDIUM
CVE-2025-24526	5.3 MEDIUM
CVE-2025-25279	5.3 MEDIUM

CWE's

CWE	Beschrijving

CWE-384	Session Fixation
CWE-863	Incorrect Authorization
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Getroffen producten

mattermost
mattermost

Disclaimer