



NCSC-2025-0378

Kwetsbaarheden verholpen in Mattermost

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 28-11-2025

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 11.0.x (tot en met 11.0.3), 10.12.x (tot en met 10.12.1), 10.11.x (tot en met 10.11.4) en 10.5.x (tot en met 10.5.12).

Duiding

De kwetsbaarheden stellen een geauthenticeerde aanvaller in staat om een account over te nemen via een zorgvuldig vervaardigd e-mailadres tijdens het authenticatieproces. Dit vereist specifieke instellingen die geconfigureerd moeten zijn, wat gebruikersaccounts bloot kan stellen aan ongeautoriseerde toegang. Daarnaast kan een geauthenticeerde aanvaller met teamcreatieprivileges de OAuth state token validatie misbruiken om een gebruikersaccount over te nemen door authenticatiegegevens te manipuleren, vooral als e-mailverificatie is uitgeschakeld.

Voor deze laatste kwetsbaarheid moet de kwaadwillende beschikken over twee accounts, waarvan er een nog niet eerder ingelogd is geweest. Misbruik is hiermee ingewikkeld te realiseren.

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-2025-12421	5.3 MEDIUM
➤ CVE-2025-12419	5.3 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-303	Incorrect Implementation of Authentication Algorithm

Getroffen producten

Mattermost

Mattermost

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.