



NCSC-2026-0305

Kwetsbaarheden verholpen in Mattermost

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 19-08-2026

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, Inc. heeft kwetsbaarheden verholpen in Mattermost versies 10.11.x, 11.7.x en 11.8.x, inclusief de GitLab plugin tot versie 11.8.

Duiding

De kwetsbaarheden betreffen meerdere aspecten van de Mattermost software, waaronder onjuiste validatie van WebSocket command velden, onjuiste reconciliatie van SchemeAdmin flags, en onvoldoende verificatie van kanaaleigendom bij ABAC policy unassign endpoints. Hierdoor kunnen geauthenticeerde gebruikers onder andere denial-of-service veroorzaken door het laten crashen van plugin processen, administratieve privileges behouden na demotie, en ongeautoriseerde wijzigingen aanbrengen in toegangscontrolebeleid en board-rollen. Verder kunnen guest gebruikers via speciaal vervaardigde boardarchiefbestanden hun privileges escaleren naar Board Admin. OAuth applicaties kunnen tokens en autorisaties van andere integraties intrekken door onvoldoende restricties op deaccountbeheer endpoints. Ook is het mogelijk om voltooid playbook runs te wijzigen door het ontbreken van run-state validatie. Daarnaast kunnen gebruikers zonder voldoende leesrechten boards koppelen aan kanalen, waardoor lidmaatschappen van private kanalen worden blootgesteld. Channel administrators kunnen hun permissies verhogen via manipulatie van de channel member roles API.

De GitLab plugin vertoont een kwetsbaarheid waardoor bots berichten met willekeurige URLs kunnen injecteren in kanalen zonder toegangsrechten. Thread membership records worden niet verwijderd bij vertrek uit een team, wat toegang tot private thread content kan geven bij herintreding. Ten slotte is er een kwetsbaarheid in de server-side validatie van BoardMember.Scheme* velden, waardoor privilege escalatie mogelijk is door het toekennen van board admin rechten aan willekeurige gebruikers, en een permissiecontrole ontbreekt bij het relinken van boards aan kanalen via de batch endpoint.

Oplossingen

Mattermost, Inc. heeft updates uitgebracht om de kwetsbaarheden te verhelpen in de genoemde versies van Mattermost en de GitLab plugin. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://mattermost.com/security-updates/>

Kwetsbaarheden

CVE	CVSS Score

➤ CVE-2026-10080	6.5 MEDIUM
➤ CVE-2026-10527	6.3 MEDIUM
➤ CVE-2026-15754	4.2 MEDIUM
➤ CVE-2026-16044	5.4 MEDIUM
➤ CVE-2026-16045	4.3 MEDIUM
➤ CVE-2026-16046	4.3 MEDIUM
➤ CVE-2026-16047	4.3 MEDIUM
➤ CVE-2026-16048	6.3 MEDIUM
➤ CVE-2026-16049	4.3 MEDIUM
➤ CVE-2026-9693	3.5 LOW
➤ CVE-2026-9816	8.3 HIGH
➤ CVE-2026-9859	6.5 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-20	Improper Input Validation
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-269	Improper Privilege Management
➤ CWE-275	Permission Issues
➤ CWE-285	Improper Authorization
➤ CWE-371	State Issues
➤ CWE-459	Incomplete Cleanup
➤ CWE-704	Incorrect Type Conversion or Cast
➤ CWE-862	Missing Authorization

[> CWE-863](#)

Incorrect Authorization

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.