CERT-EU

Security Advisory 2025-006

Critical Vulnerabilities in Mattermost

2025-03-05 — v1.0

TLP:CLEAR

History:

- *05/03/2025 — v1.0 – Initial publication*

Summary

On 23 January 2025, Mattermost used advisories for several vulnerabilities, including three critical severity flaws affecting the Board plugin [1]. If exploited, these vulnerabilities could allow an authenticated attacker to read any file on the server, or read data directly from the database.

It is recommended to check for potential abuse, and to update vulnerable Mattermost instances.

Technical Details

The vulnerability **CVE-2025-25279**, with a CVSS score of 9.9, arises due to a failure to validate board blocks during import processes. An attacker can exploit this vulnerability by importing a specially crafted archive. Upon successful exploitation, the attacker can read arbitrary files on the targeted system [2].

The vulnerability **CVE-2025-20051**, with a CVSS score of 9.9, arises due to a failure to validate user input during the patching and duplication of a board. Maliciously crafted blocks can be used to read arbitrary files on the system by an attacker [3].

The vulnerability **CVE-2025-24490**, with a CVSS score of 9.6, stems from the application's failure to utilise prepared statements in SQL queries when reordering boards categories. An attacker can exploit this vulnerability through SQL injection, gaining the ability to retrieve sensitive data from the database [4].

Products Affected

Those vulnerabilities affect Mattermost versions 10.4.x up to 10.4.1, 9.11.x up to 9.11.7, 10.3.x up to 10.3.2, and 10.2.x up to 10.2.2 where the Boards plugin is enabled.

Recommendations

CERT-EU recommends updating to the latest version of the affected Mattermost instance as soon as possible to mitigate those vulnerabilities.

For Internet facing applications, it is recommended using a Web Application Firewall (WAF) to detect or prevent most common vulnerability types exploitation [5].

Detection

To detect possible exploitations of **CVE-2025-25279** or **CVE-2025-20051**, it is possible to review the `fields` column of the table `focalboard_blocks` in the database for common LFI payloads (e.g. `../..`).

When request bodies are being logged (in HTTP or WAF logs), it is also recommended to review POST requests related to the `focalboard` API endpoint for common LFI payloads (e.g. `../..`), especially in the `fields` variable [6].

References

[1] https://mattermost.com/security-updates/

[2] https://www.recordedfuture.com/vulnerability-database/CVE-2025-25279

[3] https://www.recordedfuture.com/vulnerability-database/CVE-2025-20051

[4] https://www.recordedfuture.com/vulnerability-database/CVE-2025-24490

[5] https://owasp.org/www-project-top-ten/

[6] https://github.com/numanturle/CVE-2025-25279