MATTERMOST CRITICAL VULNERABILITIES

Vairav Advisory Report

Date: February 25, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Mattermost, an open-source team communication and collaboration platform, has patched three critical security vulnerabilities affecting its Boards plugin. These vulnerabilities (CVE-2025-20051, CVE-2025-24490, and CVE-2025-25279) could allow attackers to read arbitrary files and execute SQL injection attacks. Organizations using affected versions must update to the latest secure releases immediately.

VULNERABILITY DETAILS

CVE-2025-20051: Arbitrary File Read via Block Duplication

Description: This vulnerability allows attackers to exploit block duplication functionality in Mattermost Boards to read arbitrary files. By duplicating a specially crafted block, attackers could gain unauthorized access to sensitive data.

Impact: Information disclosure, and potential data compromise.

CVSS Score: 9.9 (Critical).

CVE-2025-24490: SQL Injection via Board Category ID Reordering

Description: Attackers can exploit this vulnerability by manipulating board category ID reordering requests, leading to unauthorized data retrieval from the Mattermost database.

Impact: Data breaches, and unauthorized access.

CVSS Score: 9.6 (Critical).

CVE-2025-25279: Arbitrary File Read via Import/Export Functionality

Description: This vulnerability allows attackers to craft malicious import archives to exploit Mattermost Boards' import/export functionality, potentially accessing sensitive system files.

Impact: Information disclosure, and unauthorized access.

CVSS Score: 9.9 (Critical)

AFFECTED VERSIONS

Mattermost version:

- before and including 10.4.1
- before and including 9.11.7
- before and including 10.3.2
- before and including 10.2.2

EXPLOIT DETAILS

Attackers can exploit these vulnerabilities remotely without authentication by sending specially crafted requests to Mattermost Boards. CVE-2025-20051 and CVE-2025-25279 allow unauthorized file access, potentially exposing sensitive configurations and internal data. CVE-2025-24490 enables SQL injection attacks, which could be used to extract or manipulate data within the Mattermost database. If successfully chained, these vulnerabilities could lead to full system compromise, data exfiltration, and lateral movement within an organization's network.

RECOMMENDED ACTIONS

- Mattermost urges users to update to the latest secure versions: 10.5.0, 10.4.2, 9.11.8, 10.3.3, 10.2.3
- Alternatively, updating the Mattermost Boards plugin to v9.0.5 or higher will mitigate these vulnerabilities.

ADDITIONAL SECURITY MEASURES

- Restrict database and file system access to prevent unauthorized exploitation.
- Apply input validation to prevent SQL injection attacks.
- Enable security monitoring to detect suspicious activity in Mattermost Boards.

REFERENCES

https://securityonline.info/critical-mattermost-flaws-cve-2025-20051-cve-2025-24490-cve-2025-25279-expose-systems-to-file-read-and-sql-injection-attacks/

https://nvd.nist.gov/vuln/detail/CVE-2025-20051

https://nvd.nist.gov/vuln/detail/CVE-2025-24490

https://nvd.nist.gov/vuln/detail/CVE-2025-25279

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

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com