مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Mattermost Boards Plugin

Tracking #:432316903

Date: 25-02-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Mattermost Boards Plugin, which could allow attackers to read arbitrary files and perform SQL injection attacks, potentially leading to significant data breaches and unauthorized access to affected systems.

TECHNICAL DETAILS:

Mattermost, an open-source platform for team communication and collaboration, has addressed three critical security vulnerabilities affecting its Boards plugin. These vulnerabilities, identified as CVE-2025-20051, CVE-2025-24490, and CVE-2025-25279, pose significant security risks, including arbitrary file reads and SQL injection attacks.

Critical-Severity Vulnerabilities:

- **CVE-2025-20051 (CVSS 9.9):**
  - Allows arbitrary file reads via block duplication in Mattermost Boards.
  - Attackers can exploit this flaw by duplicating a specially crafted block, potentially gaining access to sensitive information.
- **CVE-2025-24490 (CVSS 9.6):**
  - An SQL injection vulnerability that enables attackers to retrieve data from the Mattermost database.
  - Exploited through manipulated board category ID reordering requests, potentially leading to data breaches and unauthorized access.
- **CVE-2025-25279 (CVSS 9.9):**
  - Enables arbitrary file reads via the import and export functionality in Mattermost Boards.
  - Attackers can craft malicious import archives to exploit this flaw, potentially compromising sensitive data.

Affected Versions:

- 10.4.x <= 10.4.1
- 9.11.x <= 9.11.7
- 10.3.x <= 10.3.2
- 10.2.x <= 10.2.2

Fixed Versions:

- Mattermost 10.5.0
- Mattermost 10.4.2
- Mattermost 9.11.8
- Mattermost 10.3.3
- Mattermost 10.2.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Mattermost.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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