مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Path Traversal Vulnerability in Mattermost
Tracking #:432317737
Date:22-09-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity path traversal vulnerability has been identified in Mattermost Server, a popular open-source collaboration and messaging platform.

TECHNICAL DETAILS:

A high-severity path traversal vulnerability has been identified in Mattermost Server, a popular open-source collaboration and messaging platform. The flaw impacts multiple supported branches and arises due to insufficient validation of the import directory path configuration.

Vulnerability Details:
- **CVE ID:** CVE-2025-9079
- **CVSS v3.1 Score:** 8.7 (High)
- **Vulnerability Type:** Path Traversal / Arbitrary Code Execution
- **Affected Package:** github.com/mattermost/mattermost-server (Go) and github.com/mattermost/mattermost/server/v8
- **Affected Versions:**
  - mattermost-server
    - 10.8.0 – 10.8.3
    - 10.5.0 – 10.5.8
    - 9.11.0 – 9.11.17
    - 10.10.0 – 10.10.1
    - 10.9.0 – 10.9.3
  - mattermost/server/v8
    - Versions < 8.0.0-20250707221302-a8fa77f107ef
- **Patched Versions:**
  - 10.8.4
  - 10.5.9
  - 9.11.18
  - 10.10.2
  - 10.9.4
  - mattermost/server/v8@8.0.0-20250707221302-a8fa77f107ef
- **Attack Vector:** Network
- **Privileges Required:** High (Admin access)
- **User Interaction:** None
- **Impact:**
  - **Confidentiality:** High (data disclosure)
  - **Integrity:** High (data tampering / server takeover)
  - **Availability:** High (system compromise)

RECOMMENDATIONS:

- Apply Security Updates Immediately: Upgrade to the patched versions at the earliest.

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.

REFERNCES:

- https://github.com/advisories/GHSA-qx3f-6vq3-8j8m