

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Remote Code Execution Vulnerability in Mattermost

Tracking #:432317403

Date:23-06-2025

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Mattermost, an open-source team collaboration platform widely used by enterprises and government organizations.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-4981) has been discovered in Mattermost, an open-source team collaboration platform widely used by enterprises and government organizations. The flaw, rated CVSS 9.9, enables authenticated users to perform path traversal attacks during archive file extraction, potentially leading to remote code execution (RCE) on the host system.

The vulnerability affects multiple versions of Mattermost and stems from improper validation of file paths in uploaded compressed archives (e.g., .zip, .tar.gz). If default settings for file attachments and content extraction are enabled, malicious users can plant files in sensitive system directories, execute arbitrary code, and escalate privileges.

This issue poses a severe threat to organizations using Mattermost for internal communications, especially in sectors handling confidential data such as healthcare, finance, and government.

Vulnerability Details

- **CVE:** CVE-2025-4981
- **CVSS Score:** 9.9 (Critical)
- **Vulnerability Type:** Path Traversal → Arbitrary File Write → RCE
- **Attack Vector:** Authenticated file upload of malicious archive
- **Impact:** Remote Code Execution, Privilege Escalation, File System Compromise
- **Exploitable By:** Any authenticated user with file upload permissions

Affected Versions:

- 10.5.x ≤ 10.5.5
- 9.11.x ≤ 9.11.15
- 10.8.x ≤ 10.8.0
- 10.7.x ≤ 10.7.2
- 10.6.x ≤ 10.6.5

Fixed Versions:

- 10.9.0
- 10.8.1
- 10.7.3
- 10.6.6
- 10.5.6
- 9.11.16

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to Upgrade Mattermost to the latest secure version immediately.

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/>