CVE-2025-25068: Mattermost Server MFA bypass via API requests

Vairav CVE Report

Date: March 21st, 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

A single vulnerability **CVE-2025-25068** has been in identified in Mattermost Servers. This vulnerability allows authenticated attackers to bypass MFA protections via API requests to plugin-specific routes. It has been assigned a **CVSS score of 7.5 (High).** If exploited, these vulnerabilities could lead to unauthorized access and potential system compromise.

VULNERABILITY DETAILS

CVE-2025-25068

- **Description:** This vulnerability allows authenticated attackers to bypass MFA protections vi API requests to plugin-specific routes.
- **Impact:** If successfully exploited, attackers could gain unauthorized access to sensitive data, escalate privileges, and execute administrative actions without passing MFA checks. This increases the risk of data breaches, account takeovers, and lateral movement within the network, potentially compromising critical business operations and violating compliance requirements
- **CVSS Score:** 7.5 (High)

AFFECTED VERSIONS

The following Mattermost Server versions are affected:

- Versions 10.4.0 through 10.4.2
- Versions 10.3.0 through 10.3.3
- Versions 9.11.0 through 9.11.8
- Version 10.5.0

EXPLOIT DETAILS

This vulnerability is particularly concerning in environments where Mattermost is used as a collaboration platform. Exploitation could lead to unauthorized access to sensitive communications and data, potentially resulting in data breaches and operational disruptions.

RECOMMENDED ACTIONS

An official fix is not available yet. Patch and upgrade to the latest version once it is released.

ADDITIONAL SECURITY MEASURES

- **Restrict and Monitor Access**: Limit access to plugin endpoints using firewall rules, and monitor logs for suspicious activity.
- **Enforce MFA at Proxy**: Use a reverse proxy to enforce MFA on API requests to plugin endpoints.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-25068
- https://www.cve.org/CVERecord?id=CVE-2025-25068

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