مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in AI Engine WordPress Plugin

Tracking #:432317941

Date:05-11-2025

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 a critical vulnerability in the AI Engine WordPress plugin that allows unauthenticated attackers to escalate privileges and take full control of affected websites.

TECHNICAL DETAILS:

A critical Sensitive Information Exposure vulnerability (CVE-2025-11749) has been identified in the AI Engine WordPress plugin, allowing unauthenticated attackers to escalate privileges and gain full administrative control over affected websites.

The issue resides in the plugin's Model Context Protocol (MCP) feature when the "No-Auth URL" option is enabled, inadvertently exposing sensitive authentication tokens through the WordPress REST API.

Vulnerability Details

- **CVE-2025-11749**
- **Severity:** Critical (CVSS 9.8)
- **Affected Component:** Model Context Protocol (MCP) – "No-Auth URL" feature
- **Exploitation Status:** Active exploitation attempts observed
- The vulnerability arises from how the plugin registers REST API routes via the rest_api_init() function in the Meow_MWAI_Labs_MCP class. When the "No-Auth URL" feature is enabled, **bearer tokens** are exposed through the /wp-json/ REST API index, allowing attackers to retrieve them and **authenticate as administrators** via the MCP endpoint. This grants full access to administrative commands such as wp_update_user, enabling attackers to modify user roles, upload malicious plugins, or alter site content.

Affected Versions

- AI Engine plugin versions **<= 3.1.3**

Fixed Version

- AI Engine 3.1.4 or later

RECOMMENDATIONS:

- Update Immediately: Upgrade to version 3.1.4 or later.
- Disable "No-Auth URL": Ensure this setting is disabled unless strictly necessary.
- Revoke Tokens: Regenerate any exposed bearer tokens.
- Audit Accounts: Check for unauthorized admin users and suspicious activity.
- Enhance Protection: Use a WAF and enable MFA for all administrator accounts.

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://www.wordfence.com/blog/2025/11/100000-wordpress-sites-affected-by-privilege-escalation-vulnerability-in-ai-engine-wordpress-plugin/