مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in WordPress AI Engine Plugin

Tracking #:432317397

Date:20-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the AI Engine plugin for WordPress that could be exploited to escalate privileges and take full control of affected sites.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-5071) has been identified in the AI Engine plugin for WordPress that allows authenticated users with subscriber-level access to escalate privileges and gain full administrative control of a site.

Vulnerability Details:

- CVE-2025-5071
- CVSS Score: 8.8 High
- The issue arises when the Model Context Protocol (MCP) and Dev Tools features are enabled. Due to missing checks in the can_access_mcp() function and the mwai_allow_mcp filter, unauthorized access to backend functionality becomes possible—even when Bearer Token authentication is configured. The validation logic fails to check for empty token values, allowing logged-in users to bypass authentication.
- Once access is gained, attackers can execute the wp_update_user command to escalate privileges.
- Exploitation can lead to full site compromise, including the ability to:
  - Escalate user privileges to administrator
  - Upload malicious plugins or webshells
  - Modify or delete site content
  - Redirect users to malicious domains
  - Inject spam or phishing content

Affected Versions:

- AI Engine prior 2.8.0 – 2.8.3.

Fixed Versions:

- AI Engine plugin to version 2.8.4 or later.

RECOMMENDATIONS:

- Update the AI Engine plugin to the latest version
- Disable the Dev Tools and MCP module if not required.
- Enforce strong authentication and access control for all administrative endpoints.
- Regularly audit plugin configurations and user privileges.
- Monitor for suspicious administrative activity.

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/2025/06/100000-wordpress-sites-affected-by-privilege-escalation-via-mcp-in-ai-engine-wordpress-plugin/
- https://nvd.nist.gov/vuln/detail/CVE-2025-5071