مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Perfmatters WordPress Plugin

Tracking #:432318725
Date:06-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the Perfmatters WordPress plugin, a widely used performance optimization tool. The flaw allows unauthenticated attackers to delete arbitrary files on the server, potentially leading to full website takeover.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-4350
- **Severity:** High **CVSS Score:** 8.1
- The vulnerability in the PMCS::action_handler() function allows unauthenticated attackers to exploit a path traversal flaw due to missing input sanitization, authorization checks, and nonce verification. By crafting malicious requests, attackers can delete arbitrary files on the server, including the critical wp-config.php file. This can force the site into a setup state and enable attackers to reconfigure it, resulting in a complete site takeover.

Affected Versions

- Perfmatters WordPress Plugin
  - All versions up to, and including, 2.5.9.1

Fixed Versions

- Perfmatters WordPress Plugin
  - 2.6.0 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Vendor.

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.cve.org/CVERecord?id=CVE-2026-4350
- https://www.wordfence.com/blog/2026/04/200000-wordpress-sites-affected-by-arbitrary-file-deletion-vulnerability-in-perfmatters-wordpress-plugin/