مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

WordPress Automatic Plugin Vulnerable to SQL Injection Attacks

Tracking #:432315797
Date:29-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical severity vulnerability in the WordPress Automatic plugin. Threat actors are actively exploiting this vulnerability to gain unauthorized access to websites, create new administrator accounts, and steal sensitive information.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-27956**
- CVSS Score: 9.9 CRITICAL
- A critical security vulnerability exists in the WordPress Automatic plugin. This vulnerability is an SQL injection (SQLi) that allows an unauthenticated attacker to inject malicious SQL code into the website's database. By exploiting this vulnerability attackers can gain unauthorized access to websites, create administrator accounts, upload malicious files, and potentially take complete control of affected sites.

Impact:

- Attackers can gain unauthorized administrative access to WordPress websites.
- Attackers can install backdoors and steal sensitive information.
- Attackers can deface websites or launch further attacks.

Affected Versions:

- WordPress Automatic Plugin Versions: < 3.9.2.0

Fixed Versions:

- WordPress Automatic Plugin Versions: 3.92.1 or later

Indicators of Compromise (IoCs):

- Administrator user with name starting with **xtw.**
- The vulnerable file *"/wp-content/plugins/wp-automatic/inc/csv.php"* renamed to something as *"/wp-content/plugins/wp-automatic/inc/csv65f82ab408b3.php"*
- Presence of the following files with specific SHA1 hashes:
  - b0ca85463fe805ffdf809206771719dc571eb052 web.php
  - 8e83c42ffd3c5a88b2b2853ff931164ebce1c0f3 index.php

RECOMMENDATIONS:

- **Update Immediately:** Ensure that the WP-Automatic plugin is updated to the latest version.
- **Review User Accounts:** Regularly review and audit user accounts within WordPress, removing any unauthorized or suspicious admin users.
- **Security Monitoring:** Implement robust security monitoring tools to detect and respond to malicious activity.
- **Backups:** Maintain up-to-date backups of your website data for swift restoration in case of a compromise.

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://patchstack.com/database/vulnerability/wp-automatic/wordpress-automatic-plugin-3-92-0-unauthenticated-arbitrary-sql-execution-vulnerability?_s_id=cve
- https://wpscan.com/blog/new-malware-campaign-targets-wp-automatic-plugin/