Hackers Actively Exploiting WP Automatic Updates Plugin Vulnerability

Date: 27th April 2024 | Severity: Medium

Summary

Hackers have started to target a critical severity vulnerability in the WP Automatic plugin for WordPress to create user accounts with administrative privileges and to plant backdoors for long-term access.

Attack Vectors

- Currently installed on more than 30,000 websites, WP Automatic lets administrators automate content importing (e.g. text, images, video) from various online sources and publishing on their WordPress site. The exploited vulnerability is identified as as CVE-2024-27956 and received a severity score of 9.9/10.
- It was disclosed publicly by researchers at PatchStack vulnerability mitigation service on March 13 and described as an SQL injection issue that impacts affecting WP Automatic versions before 3.9.2.0.
- The issus is in the plugin's user authentication mechanism, which can be bypassed to submit SQL queries to the site's database. Hackers can use specially crafted queries to create administrator accounts on the target website.
- Once a WordPress site is compromised, attackers ensure the longevity of their access by creating backdoors and obfuscating the code," reads WPScan's report. Once they get control of the website, the threat actor often installs additional plugins that allow uploading files and code editing.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• b0ca85463fe805ffdf809206771719dc571eb052 • 8e83c42ffd3c5a88b2b2853ff931164ebce1c0f3
File name	• /wp-content/plugins/wp-automatic/inc/csv65f82ab408b3[.]php
Accountname	• admin account starting with "xtw"

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Make sure to keep the WP-Automatic plugin updated to the latest version to patch any known vulnerabilities and ensure security.
- Regularly audit WordPress user accounts to remove unauthorized or suspicious admin users, which helps reduce the risk of unauthorized access.
- Always utilize robust security monitoring tools like Jetpack Scan to detect and respond to malicious activity promptly.
- Maintain up-to-date backups of your website data to enable quick restoration in case of a compromise, ensuring minimal downtime and data loss.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.bleepingcomputer.com/news/security/wp-automatic-wordpress-plugin-hit-by-millions-of-sql-injection-attacks/
- Hackers Actively Exploiting WP Automatic Updates Plugin Flaw (cybersecuritynews.com)