Smarttech
YOUR 24/7 SECURITY PARTNER

Threat Report

Actively exploited critical vulnerability found in WordPress Automatic Plugin

Document ID	SMA- Threat Report
Document status	ISSUED
Issue Number	02
Authors	Oana Nitu <oana.nitu@smarttech247.com>
Verified by	Alin Curcan <alin.curcan@smarttech247.com>
Last modified	2024-04-25
Issue Date	2024-04-25

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e., vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed, and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time, and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

A security vulnerability in the WP Automatic WordPress plugin, identified as CVE-2024-27956, has exposed millions of websites to SQL injection attacks. The plugin, which automates content publishing on WordPress websites, is being targeted by hackers who are exploiting the flaw to inject malicious code and take control of affected sites.

The vulnerability poses a significant risk to website owners using the WP Automatic plugin and highlights the importance of regularly updating plugins and maintaining strong security practices. Security experts have warned users to be vigilant and take immediate action to mitigate the impact of potential attacks.

RISK

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

TECHNICAL SUMMARY

CVE-2024-27956| WordPress Automatic plugin <= 3.92.0 - Unauthenticated Arbitrary SQL Execution vulnerability

CVSS Base Score: 9.9

A critical vulnerability in the WP Automatic plugin presents a significant risk, enabling attackers to gain unauthorized entry into websites, establish admin-level user accounts, upload harmful files, and potentially assume complete control over targeted sites.

This vulnerability stems from the WP-Automatic plugin's mishandling of user authentication mechanisms within one of its files. Attackers can exploit this flaw to circumvent security measures and execute malicious SQL queries.

Exploitation Steps:

- SQL Injection (SQLi): Utilizing the SQLi flaw in the WP-Automatic plugin, attackers execute unauthorized database queries.
- Admin User Creation: With the capability to execute arbitrary SQL queries, attackers generate new admin-level user accounts within WordPress.
- Malware Upload: Upon successfully creating an admin-level account, attackers upload malicious files, often web shells or backdoors, onto the server of the compromised website.
- File Renaming: Attackers may opt to rename the vulnerable WP-Automatic file to ensure exclusive exploitation privileges.

This vulnerability was publicly disclosed on March 13, 2024, and since then, records indicate a staggering 5,576,488 attempted attacks. The campaign initially unfolded slowly but surged to its peak on March 31st.

Systems Affected:

The CVE-2024-27956 vulnerability affects WP-Automatic plugin versions 3.92.0 and prior.

Fixed versions:

A complete patch was released when WP Automatic plugin version 3.92.1 was rolled out.

Indicators of compromise:

If any of the following indicators are found in the environment it means that the site in question was compromised by this active campaign:

- 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"
- The following SHA1 hashed files dropped in your site's filesystem:

  b0ca85463fe805ffdf809206771719dc571eb052 web.php
  8e83c42ffd3c5a88b2b2853ff931164ebce1c0f3 index.php

Recommendations

Smarttech247 team **highly** recommends the following actions be taken:

- **Plugin Updates:** Ensure the WP-Automatic plugin is kept up to date with the latest version.
- **User Account Management:** Regularly review and audit user accounts in WordPress, removing any unauthorized or suspicious admin users.
- **Security Monitoring:** Utilize robust security monitoring tools like Jetpack Scan to detect and respond to malicious activity on your website. Consider enabling Enhance Protection within Jetpack Scan to bolster your website's security. This feature enables the Web Application Firewall (WAF) to scrutinize requests aimed at standalone PHP files, even those vulnerable to attack. Thus, it offers protection against potential threats by inspecting and safeguarding your website against such attempts.
- **Backup and Recovery:** Maintain current backups of your website data to facilitate rapid restoration in case of a compromise.

References

https://www.bleepingcomputer.com/news/security/wp-automatic-wordpress-plugin-hit-by-millions-of-sql-injection-attacks/
https://wpscan.com/blog/new-malware-campaign-targets-wp-automatic-plugin/
https://patchstack.com/database/vulnerability/wp-automatic/wordpress-automatic-plugin-3-92-0-unauthenticated-arbitrary-sql-execution-vulnerability?_s_id=cve

CVE:

CVE-2024-27956