April 29, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware WordPress published a security advisory to address vulnerabilities in the following product:

- WP Automatic versions before 3.9.2.0.

Technical Details

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.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-27956
- WP Automatic WordPress plugin hit by millions of SQL injection attacks (bleepingcomputer.com)