January 25, 2024

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that WordPress published security advisories to address vulnerabilities. Included were critical updates for the following:

- PHP Object Injection in all versions up to, and including, 1.4.4

Technical Details

The Better Search Replace plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.4 via deserialization of untrusted input. This makes it possible for unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.

Wordfence blocked **2,591 attacks** targeting this vulnerability in the past 24 hours.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-6933
- Better Search Replace <= 1.4.4 - Unauthenticated PHP Object Injection (wordfence.com)