Security Advisory 2023-096

High Severity Vulnerability in WordPress

December 11, 2023 — v1.0

TLP:CLEAR

History:

- *11/12/2023 — v1.0 – Initial publication*

Summary

On December 6, 2023, WordPress released a new version addressing a vulnerability that, if combined with another vulnerability, could result in remote code execution [1].

While most sites should automatically update to WordPress 6.4.2, it is strongly recommended manually checking WordPress sites to ensure that it is updated.

Technical Details

The vulnerability is a property-oriented programming (POP) chain issue identified in a class introduced to improve HTML parsing in the block editor. The vulnerable class includes a function that is executed automatically after PHP has processed a request, and which uses properties that an attacker may have full control of [2].

It can be combined with a different object injection flaw, allowing attackers to execute PHP code on vulnerable websites. While WordPress Core currently does not have any known object injection vulnerabilities, the WordPress security team feels that there is potential for high severity when combined with some plugins, especially in multi-site installations.

Affected Products

This vulnerability affects WordPress version 6.4 until 6.4.2 (excluded).

Recommendations

It is strongly recommended manually checking WordPress sites to ensure that it is updated, and if not, It is strongly recommended updating it.

References

[1] https://wordpress.org/documentation/wordpress-version/version-6-4-2/

[2] https://www.wordfence.com/blog/2023/12/psa-critical-pop-chain-allowing-remote-code-execution-patched-in-wordpress-6-4-2/

[3] https://www.securityweek.com/wordpress-6-4-2-patches-remote-code-execution-vulnerability/