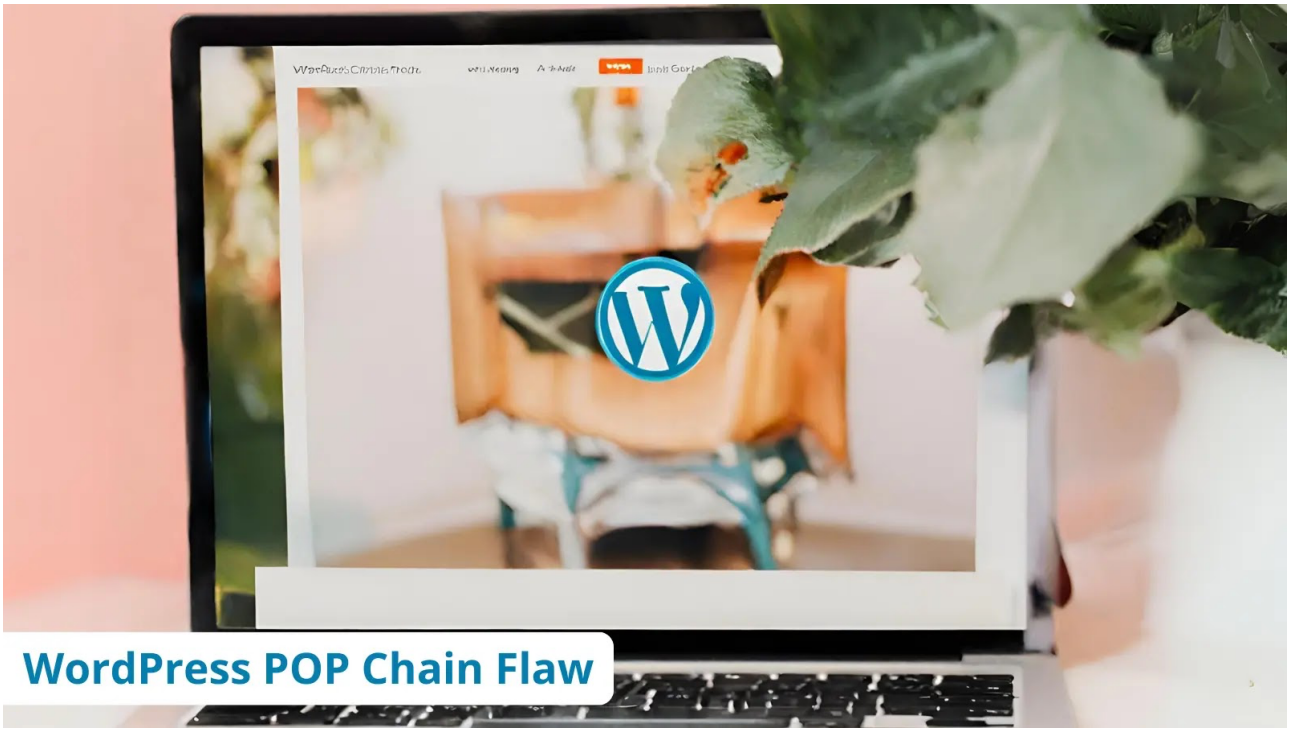
WordPress POP Chain Flaw Exposes Over 800M+ Websites To Attack

December 9, 2023 By **Guru Baran**



A critical remote code execution vulnerability has been patched as part of the WordPress 6.4.2 version.

This vulnerability exists in the POP chain introduced in version 6.4, which can be combined with a separate Object Injection, resulting in the execution of arbitrary PHP code on the website.

There was no CVE assigned for this vulnerability. However, WordPress urges its users to upgrade to this latest version to prevent full site takeover attacks in case another vulnerability exists.

WordPress POP Chain Flaw

This vulnerability exists in the WP_HTML_Token class, which is used to improve HTML parsing in the block editor.

This class contains a __destruct method that gets executed automatically when the PHP has processed the request. It also uses call_user_func to execute the function passed to the on_destroy property.

A threat actor can take full control over the on_destroy and bookmark_name properties by exploiting an Object Injection vulnerability and executing arbitrary code on the website.

```
public function __wakeup() {
  throw new \LogicException( __CLASS__ . ' should never be unserialized' );
}
```

Source: *WordPress*

Moreover, there is a potential POP chain in the WordPress core that can increase the risk of any Object Injection vulnerabilities. However, the current version of WordPress' newly added __wakeup method uses a serialized object with the WP_HTML_Token class that prevents the __destruct function from executing.

A complete report about this vulnerability has been published by Wordfence, which provides detailed information about the source code, analysis, and other information.

Users of WordPress are recommended to upgrade to the latest version 6.4.2, to prevent this vulnerability from getting exploited by threat actors.

To install the latest version of WordPress, a complete guide with a step-by-step procedure has also been provided.