Security Advisory 2022-012

Critical Vulnerabilities in PHP Everywhere WordPress Plugin

February 11, 2022 — v1.1

TLP:WHITE

History:

- *10/02/2022 — v1.0 – Initial publication*
- *11/02/2022 — v1.1 – Fix the links in the references*

Summary

On January 4th, researchers found three critical 'PHP Everywhere' plugin for WordPress. These vulnerabilities identified as `CVE-2022-24663`, `CVE-2022-24664` and `CVE-2022-24665` affect many WordPress sites and can lead to **remote code execution (RCE)** that could be leveraged to achieve a complete site takeover. All three have a CVSS score of 9.9.

The vulnerabilities were found on January 4th, but due to the responsible disclosure process, the information about them has been publicly published 30 days after the release of patched version. No proof-of-concept or ongoing exploitation of these vulnerabilities have been observed yet. However, it is highly recommended to apply the patches as soon as possible [1].

Technical Details

PHP Everywhere is a plugin that allows WordPress admins to insert PHP code into pages, posts, the sidebar, or any Gutenberg block, and use it to display dynamic content based on evaluated PHP expressions [2].

With the `CVE-2022-24663` vulnerability, any logged-in user, even a user with almost no permissions, such as a Subscriber or a Customer, is able to execute arbitrary PHP on a site by sending a request with the `shortcode` parameter set to `[php_everywhere]<arbitrary PHP>[/php_everywhere]`.

The `CVE-2022-24664` vulnerability consists of default rights for all users with the `edit_posts` capability to use the PHP Everywhere metabox. This means that untrusted Contributor-level users could use the PHP Everywhere metabox to achieve code execution on a site by creating a post, adding PHP code to the PHP Everywhere metabox, and then previewing the post. While this vulnerability has the same CVSS score as the shortcode vulnerability above, it is less severe, since it requires contributor-level permissions, which imply some degree of trust and are more difficult to obtain than subscriber-level permissions.

The last vulnerability - `CVE-2022-24665` - is pretty similar to the metabox one but this time with the PHP Everywhere Gutenberg block. Contributor-level users could execute arbitrary PHP code

on a site by creating a post, adding the PHP everywhere Gutenberg block and adding code to it, and then previewing the post [1].

Affected Products

PHP Everywhere plugins versions <= 2.0.3

Recommendations

A version 3.0.0 of the plugin has been released. Upgrade to this newest version in order to avoid exploitation.

References

[1] https://www.wordfence.com/blog/2022/02/critical-vulnerabilities-in-php-everywhere-allow-remote-code-execution/

[2] https://www.bleepingcomputer.com/news/security/php-everywhere-rce-flaws-threaten-thousands-of-wordpress-sites/