Critical Vulnerabilities in PHP Everywhere Allow Remote Code Execution
Wordfence

Ram Gall

February 8, 2022

Critical Vulnerabilities in PHP Everywhere Allow Remote Code Execution

On January 4, 2022, the Wordfence Threat Intelligence team began the responsible disclosure process for several Remote Code Execution vulnerabilities in PHP Everywhere, a WordPress plugin installed on over 30,000 websites. On these vulnerabilities allowed *any* authenticated user of any level, even subscribers and customers, to execute code o site with the plugin installed. As the vulnerabilities were of critical severity, we contacted the WordPress plugin reposi with our disclosure in addition to initiating outreach to the plugin author.

We received a response from the plugin author within a few hours and sent over the full disclosure at that time. A lar rebuilt version of the plugin was made available on January 10, 2022.

Wordfence Premium users received a firewall rule protecting against these vulnerabilities the same day, on January 2022.

We recently launched Wordfence Care and Response. These two new products also receive real-time threat intellige updates, but had not yet been launched on January 4th. Wordfence Care and Wordfence Response customers recei the firewall rule immediately upon subscription and will continue to receive firewall rules and other real-time threat intelligence as soon as it is released.

Sites still using the free version of Wordfence received the same protection 30 days after the initial release, on Febru 3, 2022.

What should I do if I’m running PHP Everywhere?

If you're using the PHP everywhere plugin, it is imperative that you upgrade to the newest version, which is 3.0.0 at th
time of this writing, in order to prevent your site from being exploited. Unfortunately version 3.0.0 only supports PHP

solution. You should not continue to run older versions of PHP Everywhere under any circumstances.

Description: Remote Code Execution by Subscriber+ users via shortcode
Affected Plugin: PHP Everywhere
Plugin Slug: php-everywhere
Plugin Developer: Alexander Fuchs
Affected Versions: <= 2.0.3
CVE ID: CVE-2022-24663
CVSS Score: 9.9(Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.0.0

PHP Everywhere is a WordPress plugin that is intended to allow site owners to execute PHP code anywhere on their s
It included functionality that allowed execution of PHP Code Snippets via WordPress shortcodes. Unfortunately, WordPress allows any authenticated users to execute shortcodes via the `parse-media-shortcode` AJAX action, and some plugins also allow unauthenticated shortcode execution. As such it was possible for any logged-in user, even a user with almost no permissions, such as a Subscriber or a Customer, to execute arbitrary PHP on a site by sending a request with the `shortcode` parameter set to `[php_everywhere]<arbitrary PHP>[/php_everywhere]`. Executing arbitrary PHP on a site typically allows complete site takeover.

Description: Remote Code Execution by Contributor+ users via metabox
Affected Plugin: PHP Everywhere
Plugin Slug: php-everywhere
Plugin Developer: Alexander Fuchs
Affected Versions: <= 2.0.3
CVE ID: CVE-2022-24664
CVSS Score: 9.9(Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.0.0

By default, the PHP Everywhere plugin allowed all users with the `edit_posts` capability to use the PHP Everywhere metabox.

Unfortunately this meant that untrusted Contributor-level users could use the PHP Everywhere metabox to achieve c
execution on a site by creating a post, adding PHP code to the PHP Everywhere metabox, and then previewing the pc
While this vulnerability has the same CVSS score as the shortcode vulnerability, 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. This is due to the CVSS scoring system which does not allow "Medium" in the "Privileges Required" fielc

Description: Remote Code Execution by Contributor+ users via gutenberg block
Affected Plugin: PHP Everywhere
Plugin Slug: php-everywhere
Plugin Developer: Alexander Fuchs
Affected Versions: <= 2.0.3
CVE ID: CVE-2022-24665
CVSS Score: 9.9(Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 3.0.0

By default, the PHP Everywhere plugin allowed all users with the `edit_posts` capability to use the PHP Everywhere Gutenberg block. While it was possible to set this to admin-only, this was not set by default due to versions <= 2.0.3 r
being able to add capability checks without disabling the Gutenberg Block editor. We worked with the plugin author tc
overcome this limitation when we sent our disclosure.

Unfortunately this meant that contributor-level users could execute arbitrary PHP code on a site by creating a post, adding the PHP everywhere block and adding code to it, and then previewing the post. As with the metabox vulnerabi
this has the same CVSS score as the shortcode vulnerability but is less severe as it requires Contributor-level permissions to exploit.

Timeline

January 4, 2022 – We release a firewall rule available to Wordfence Premium, Wordfence Care, and Wordfence Response customers. We begin the disclosure process with the plugin author and disclose to the WordPress plugin

January 10, 2022 – A Patched version, 3.0.0, is released.
February 3, 2022 – The firewall rule becomes available to free Wordfence users.

Conclusion

In today's article, we discussed a set of vulnerabilities in the PHP Everywhere plugin which could be used for complet site takeover.

Sites running Wordfence Premium received a firewall rule on January 4, 2022, and Wordfence Care and Wordfence Response customers received the same firewall rule upon subscription. Sites still running Wordfence Free received tl same protection 30 days after the initial release, on February 3, 2022.

If you are running this plugin, we urge you to upgrade to the latest version immediately. If you believe your site has be compromised as a result of this vulnerability, we offer Incident Response services via Wordfence Care. If you need yc site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands-on support in case you need further assistance.

If you know anyone running this plugin we strongly advise forwarding this advisory to them, as these vulnerabilities a very easy to exploit and can be used to quickly and completely take over a site.

Did you enjoy this post? Share it!

Comments

No Comments

Wordfence Free
Wordfence Premium
Wordfence Central

Documentation
Learning Center

Blog
In The News

About Wordfence
Careers
CVE Request Form

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

□ By checking this box I agree to the terms of service and privacy policy.*

SIGN UP