Hive Pro

THREAT ADVISORY

Critical Remote Code execution vulnerabilities in WordPress PHP everywhere Plugin

TA2022027

Threat Level RED

Publish Date – Feb 10, 2022

Three critical remote code execution (RCE) vulnerabilities in a WordPress plugin PHP everywhere have been discovered. It is a plugin that allows web developers to utilize PHP code in pages, posts, the sidebar, or anywhere on domains that use the content management system (CMS). This plugin has been installed on over 30,000 websites.

The first vulnerability which has been assigned CVE-2022-24663, allows an authorized attacker to execute shortcodes via the parse-media-shortcode AJAX call. In this case, if users are signed in then even if they have absolutely no access, such as a subscriber, a forged request parameter might be provided to run arbitrary PHP code, resulting in full website takeover.

The second RCE vulnerability has been assigned CVE-2022-24664. This flaw was discovered in the way PHP Everywhere controls metaboxes, draggable edit boxes and how the software allows any user with the edit posts capability to access these functionalities. Untrusted contributor-level users might use the PHP Everywhere metabox to execute code on a site by generating a post, inserting PHP code into the PHP Everywhere metabox, and previewing the post. While this vulnerability has the same severity as the shortcode vulnerability, it is less severe because contributor-level permissions are required.

The third vulnerability is tracked as CVE-2022-24665. An attacker could tamper a website's functionality by executing arbitrary PHP code through 'edit_posts' permissions of PHP Everywhere Gutenberg blocks.

These vulnerabilities have been fixed in version 3.0.0.
Potential MITRE ATT&CK TTPs are:
TA0040: Impact
TA0001: Initial Access
TA0002: Execution
TA0007: Discovery
TA0003: Persistence
T1190: Exploit-public facing application
T1518: Software Discovery
T1565: Data Manipulation
T1059: Command and Scripting Interpreter
T1505: Server Software Component
T1505.003: Server Software Component: Web Shell

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-24663	PHP Everywhere plugin versions up to 2.0.3	cpe:2.3:a:php_everywhere_project:php_everywhere:-:*:*:*:*:wordpress:*:*	Remote Code Execution by Subscriber+ users via shortcode	CWE-94
CVE-2022-24664			Remote Code Execution by Contributor+ users via metabox	CWE-94
CVE-2022-24665			Remote Code Execution by Contributor+ users via gutenberg block	CWE-94

Patch Link

https://downloads.wordpress.org/plugin/php-everywhere.3.0.0.zip

References

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