Abandoned WordPress Plugin Abused for Backdoor Deployment

Threat actors are installing the abandoned Eval PHP plugin on compromised WordPress sites and using it to inject malicious PHP code into web pages, WordPress security company Sucuri warns.

An old plugin that has not been updated for over a decade, Eval PHP allows for the injection of PHP code into pages and posts. The code is executed whenever the injected page or post is opened in a browser.

Despite its age, the Eval PHP plugin continues to be available through the WordPress repository, and its use has spiked starting at the end of March 2023, jumping from roughly 40 installations to more than 100,000 within weeks, Sucuri reports.

This spike, the security firm explains, is associated with a malicious campaign in which threat actors are using the plugin to infect compromised websites. Eval PHP allows the attackers to drop the malicious code in multiple posts that are saved as drafts and remain hidden.

The PHP backdoor, Sucuri explains, can hide requests as cookies, which allows it to remain unnoticed.

“In all cases, attackers were able to successfully log into WordPress admin. And the malicious pages are created with a real site administrator as their author. However, on some of the compromised sites we found malicious admin users with

random names and outlook.com emails," Sucuri explains.

The dropped code "uses the file_put_contents function to create a PHP script into the docroot of the website with the specified remote code execution backdoor. All the attacker needs to do is to visit one of the infected posts or pages and the backdoor will be injected into the file structure."

By using this approach instead of dropping conventional PHP backdoors, the attackers can reinfect a compromised website when necessary, while remaining hidden: all they need to do is visit a site page.

The issue that this campaign has brought into the spotlight, Sucuri notes, is the need to re-evaluate old plugins that have been abandoned and which pose a security risk.

"Keeping such plugins in the official repository makes it easier for hackers to stay under radar since they can install a legitimate unmodified plugin from a reputable source instead of installing fake plugins or modifying existing plugins, which can be detected by scanners that monitor integrity of known plugins," Sucuri notes.

Related: Elementor Pro Plugin Vulnerability Exploited to Hack WordPress Websites

Related: Vulnerability in Popular Real Estate Theme Exploited to Hack WordPress Websites

Related: Critical Vulnerability in Premium Gift Cards WordPress Plugin Exploited in Attacks

Abandoned WordPress Plugin Abused for Backdoor Deployment