BOLETÍN DE ALERTA

Boletín Nro.: 2023-18
Fecha de publicación: 02/05/2023

Tema: Explotación activa del *plugin* Eval PHP de WordPress

El producto afectado es:

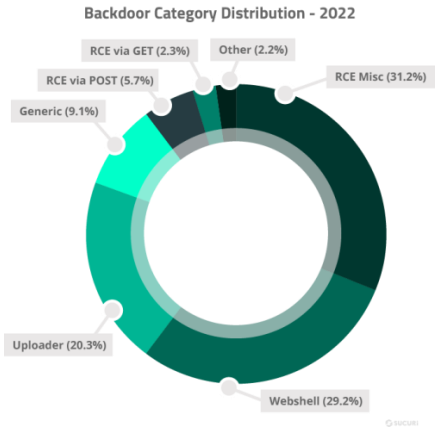
- *Plugin* Eval PHP.

Descripción:

Investigadores han descubierto una nueva campaña de *malware* explotada activamente a través del *plugin* Eval PHP que impacta a sitios web de WordPress que se hayan comprometido previamente por un atacante. Esto permitiría a un atacante la instalación de *backdoors* en el sitio comprometido a través de *scripts* PHP a través del *plugin* vulnerable y obsoleto, para posterior obtención de acceso no autorizado y toma del control del sitio, incluso después de que el administrador del sitio web haya cambiado las credenciales de administración del gestor de contenido.

El *plugin* Eval PHP no ha recibido una actualización en 11 años, las estadísticas recopiladas por WordPress muestran que está instalado en más de 8,000 sitios web, y el número aumentó en gran medida desde septiembre de 2022 al 30 de marzo de 2023. Tal cantidad de descarga llevó a la conclusión de que el ataque consiste en utilizar el *plugin* Eval PHP en sitios web de WordPress que se encuentren comprometidos y utilizarlo para establecer *backdoors* persistentes a través de múltiples *posts,* que muchas veces son guardados simplemente como borradores. El código PHP es ejecutado cada vez que el atacante o algún usuario accede a la página o publicación infectada, generando así una reinfección al descargarse nuevamente la *backdoor* completa.

Es sabido que la mayoría de las *backdoors* de sitios web se encuentran codificadas en el lenguaje de programación PHP, siendo WordPress en gran medida representante de más del 40% de las webs se encuentran basados en PHP. Según los informes del 2022 Website Threat Report, las *backdoors* de ejecución remota de código (*RCE*), *webshells* y *uploaders* son los más populares entre los atacantes para desplegarse en entornos infectados:



Fuente: https://blog.sucuri.net/2023/04/massive-abuse-of-abandoned-evalphp-wordpress-plugin.html

Detección:

Según los informes, se ha observado que las bases de datos de los sitios web afectados fueron inyectadas con códigos especialmente diseñados en la tabla *wp_posts*. Ésta tabla es la encargada de almacenar las publicaciones, páginas e información del menú de navegación de un sitio web. Dicho código es considerado bastante simple, ya que utiliza la función *file_put_contents* para crear un *script PHP* en la *docroot* del sitio web con *backdoor* de ejecución remota de código (*RCE*) especificada.

Tal inyección es una *backdoor* convencional en la estructura de archivos, sin embargo aprovecha la combinación de un *plugin* legítimo y un *backdoor dropper* en un *post* de WordPress, permitiendo de esta forma a los atacantes reinfectar fácilmente el sitio web comprometido y permanecer ocultos sin levantar sospechas. Lo que debe hacer el atacante es visitar uno de los *posts* o páginas infectadas y el *backdoor* se inyectará nuevamente en la estructura de archivos.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante con acceso privilegiado, ejecutar código PHP en la base de datos, añadir páginas falsas al sitio web oficial que se encuentra comprometido, y tomar el control de este.

Mitigación:

Recomendamos la protección del panel wp-admin de su entorno WordPress, así como la supervisión de cualquier actividad de administrador que pudiese ser sospechosa. Además de realizar regularmente la limpieza de archivos y el cambio de contraseñas, revisar los usuarios y páginas de WordPress, ya que estos podrían haber sido creados por un atacante.

Adicionalmente, recomendamos las siguientes medidas de mitigación:

- Mantener el sitio web parchado y actualizado con las últimas versiones de seguridad.
- Implementar autenticación de 2 factores (*2FA*) o algún otro método de restricción de acceso para el panel de administración del sitio web.
- Utilizar el servicio de copia de seguridad regularmente para el sitio web.
- Utilizar *firewall* de aplicaciones web para bloquear *bots* maliciosos y parchar virtualmente vulnerabilidades conocidas.
- Finalmente, en caso de sospechar que su sitio web se encuentre comprometido a algún *malware*, WordPress distribuye una herramienta para removerlo. Más información aquí.

Información adicional:

- https://thehackernews.com/2023/04/hackers-exploit-outdated-wordpress.html
- https://blog.sucuri.net/2023/04/massive-abuse-of-abandoned-evalphp-wordpress-plugin.html
- https://sucuri.net/website-malware-removal/