BOLETÍN DE ALERTA

Boletín Nro.: 2023-01
Fecha de publicación: 04/01/2023
Tema: Sitios de WordPress bajo ataque de un troyano de Linux.

Algunos temas y plugins afectados son:

- WP Live Chat Support.
- Yuzo Related Posts.
- Yellow Pencil Visual CSS Style Editor.
- Easy WP SMTP.
- WP GDPR Compliance.
- Newspaper.
- Thim Core.

Puede acceder a la lista completa de los productos afectados en el siguiente enlace.

Descripción:

Investigadores han descubierto un programa troyano (*backdoor trojan*) en Linux (versiones de 32 y 64 bits) que afecta a múltiples *plugins* y *complementos* de WordPress. Este troyano afecta a los sitios web que utilizan versiones obsoletas o desactualizadas de determinados *plugins.* Un atacante podría realizar inyección de comandos *JavaScripts* y provocar que el usuario sea redireccionado a otro sitio especialmente diseñado.

A través de un análisis del troyano se identificaron dos iteraciones del mismo, denominadas *Linux.BackDoor.WordPressExploit.1* y *Linux.BackDoor.WordPressExploit.2*. Las mismas intentan explotar vulnerabilidades en los complementos y temas de *WordPress*. Si una o más vulnerabilidades se explotan con éxito, en la página web se inyecta un código *JavaScript* malicioso que se descarga desde un servidor remoto, con el fin de que los usuarios que hagan clic en cualquier parte de dicha página infectada sean redirigidos al sitio web del atacante. Algunas de las vulnerabilidades que son utilizadas por este troyano son:

- CVE-2016-10972, de severidad “crítica”, con puntuación de 9.8. Esta vulnerabilidad se debe a un error de control en *td_ajax_update_panel* de WordPress. Que permitiría a un atacante obtener acceso no autorizado y poner en peligro el sitio web afectado.

- CVE-2019-17232, de severidad “alta”, con puntuación de 7.5. Esta vulnerabilidad se debe a un error de control en el archivo *functions/EWD_UFAQ_Import.php* del *plugin ultimate-faqs* de WordPress. Que permitiría a un atacante obtener acceso no autorizado para importar opciones que podrían poner en peligro el sitio web afectado.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar inyección de comandos *JavaScript*, redirigiendo al usuario a un sitio web especialmente diseñado con el fin de obtener información confidencial o distribuir programas maliciosos (*malware*).

Detección:

Para detectar que el sitio fue vulnerado se debe tener en cuenta los siguientes indicadores de compromiso:

- Las páginas web infectadas actúan como redireccionamientos a páginas especialmente diseñadas y controladas por el atacante, en la cual siempre cargan primero el código *JavaScript* malicioso, independientemente del contenido original del sitio.
- Estas redirecciones sirven para campañas de phishing, distribución de *malware* y publicidad maliciosa. Además, los atacantes podrían utilizar dichas páginas para vender sus servicios a otros grupos de amenazas.
- Tener en cuenta los indicadores de compromiso detallados por los investigadores en el enlace.

Solución:

Recomendamos a los administradores de sus sitios web de WordPress mantener todos sus *plugins* actualizados. Adicionalmente es necesario realizar un escaneo de vulnerabilidades regularmente a sus sitios web y tomar medidas para solucionar cualquier vulnerabilidad que sea descubierta.

Información adicional:

- https://www.darkreading.com/attacks-breaches/wordpress-under-attack-from-new-linux-backdoor-malware
- https://news.drweb.com/show/?i=14646&lng=en&c=23
- https://vms.drweb.com/virus/?i=25604695
- https://vms.drweb.com/virus/?i=25604745
- https://nvd.nist.gov/vuln/detail/CVE-2019-17232
- https://nvd.nist.gov/vuln/detail/CVE-2016-10972
- https://cyware.com/news/over-30-wordpress-plugins-and-themes-can-be-abused-by-new-linux-malware-8fbd82e6