Durante el mes de septiembre de 2023, se han comprometido más de 17,000 sitios web de WordPress con un malware conocido como Balada Injector, casi el doble de las detecciones realizadas en agosto.

De estos sitios, se informa que aproximadamente 9,000 fueron infiltrados mediante la explotación de una vulnerabilidad de seguridad recientemente divulgada en el complemento tagDiv Composer (CVE-2023-3169, puntuación CVSS: 6.1), la cual podría ser utilizada por usuarios no autenticados para llevar a cabo ataques de script entre sitios almacenados (XSS).

El investigador de seguridad de Sucuri, Denis Sinegubko, señaló que *«no es la primera vez que el grupo Inyector Balada se enfoca en vulnerabilidades de los temas premium de tagDiv».*

> *«Uno de los primeros casos masivos de inyección de malware que pudimos atribuir a esta campaña ocurrió durante el verano de 2017, cuando se abusaron activamente de vulnerabilidades divulgadas en los temas de WordPress Newspaper y Newsmag».*

El Inyector Balada es una operación a gran escala que fue identificada por primera vez por Doctor Web en diciembre de 2022, en la que los actores de amenazas explotan diversas vulnerabilidades en complementos de WordPress para instalar un backdoor de Linux en sistemas vulnerables.

El principal propósito de este implante es redirigir a los usuarios de los sitios comprometidos hacia páginas de soporte técnico falsas, estafas de premios de lotería fraudulentos y estafas de notificaciones push. Desde 2017, la campaña ha afectado a más de un millón de sitios web.

Los ataques relacionados con el Inyector Balada se desarrollan en forma de oleadas de actividad recurrente que tienen lugar cada pocas semanas, con un aumento en las infecciones detectado los martes, tras el inicio de una oleada durante el fin de semana.

En el conjunto más reciente de brechas, se ha aprovechado la vulnerabilidad CVE-2023-3169 para inyectar un script malicioso y, en última instancia, establecer un acceso persistente en los sitios mediante la carga de backdoors, la adición de complementos maliciosos y la creación de administradores de blogs falsos.

Históricamente, estos scripts se han dirigido a los administradores de sitios web de WordPress que han iniciado sesión, ya que permiten al atacante llevar a cabo acciones maliciosas con privilegios elevados a través de la interfaz de administración, incluyendo la creación de nuevos usuarios administradores que pueden utilizar para ataques posteriores.

La naturaleza en constante evolución de estos scripts se manifiesta en su capacidad para insertar un backdoor en las páginas de error 404 de los sitios web, lo que les permite ejecutar código PHP arbitrario. Además, también pueden aprovechar el código incrustado en las páginas para instalar de manera automatizada un complemento malicioso wp-zexit.

Sucuri describió esto como *«uno de los tipos de ataques más complejos»* realizados por el script, ya que simula todo el proceso de instalación de un complemento desde un archivo ZIP y su activación.

La función principal del complemento es similar a la del backdoor, que consiste en ejecutar código PHP enviado de forma remota por los actores de amenazas.

Las oleadas de ataques más recientes, observadas a finales de septiembre de 2023, involucran el uso de inyecciones de código aleatorio para descargar e iniciar un malware de segunda etapa desde un servidor remoto con el fin de instalar el complemento wp-zexit.

También se utilizan scripts ofuscados que transmiten las cookies del visitante a una URL controlada por los actores y obtienen a cambio un código JavaScript no especificado.

> Sinegubko explicó que *«la ubicación de estos scripts en los archivos de los sitios comprometidos muestra claramente que, en esta ocasión, en lugar de aprovechar*

> *la vulnerabilidad de tagDiv Composer, los atacantes utilizaron sus backdoors y usuarios administradores maliciosos que habían sido insertados después de exitosos ataques contra los administradores de los sitios web».*