BOLETÍN DE ALERTA

Boletín Nro.: 2022-05

Fecha de publicación: 25/01/2022

Tema: Investigadores descubren puerta trasera en plugins y temas de WordPress.

Software afectado:

Temas de WordPress principales afectados

- **accessbuddy versión 1.0.0**
- **accesspress-basic versión 3.2.1**
- **accesspress-lite versión 2.92**
- **accesspress-mag versión 2.6.5**

Plugins de WordPress principales afectados

- **accesspress-anonymous-post versión 2.8.0**
- **accesspress-custom-css versión 2.0.1**
- **accesspress-custom-post-type versión 1.0.8**
- **accesspress-facebook-auto-post versión 2.1.3**

Se puede acceder al listado completo de plugins y temas afectados aquí.

Descripción:

Investigadores han descubierto un *backdoor* en distintos *plugins* y temas de *AccessPress* para WordPress, descargados de sus fuentes originales, a través de un ataque a la cadena de suministro a *AccessPress*. Este código malicioso crea una puerta trasera que otorgaría a los atacantes control administrativo total sobre los sitios web que usaban los 40 temas y 53 complementos afectados pertenecientes a la tienda AccessPress. Los temas y plugins de AccessPress que estan disponible en WordPress.org no fueron afectados por el ataque.

La vulnerabilidad identificada como CVE-2021-24867, aún sin puntuación, se debe a que el archivo llamado *inital.php* que contiene un *dropper* para una webshell, el cual se encuentra ubicado en el directorio principal del plugin o tema. Cuando se ejecuta el *inital.php* se instala una cookie basada en la webshell en el archivo *wp-includes/vars.php.* La webs*hell* se ejecuta como una función llamada *wp_is_mobile_fix() en dicho archivo.* Un atacante podría obtener el control total del sitio vulnerable utilizando esta función.

Impacto:

Un atacante podría obtener el control total del sitio afectado utilizando la función que llama a la *webshell*.

Detección:

La siguiente regla YARA se puede utilizar para comprobar si el sitio es vulnerable:

```
rule accesspress_backdoor_infection

{

strings:


   // IoC's for the dropper

   $inject0 = "$fc = str_replace('function wp_is_mobile()',"

   $inject1 = "$b64($b) . 'function wp_is_mobile()',"

   $inject2 = "$fc);"

   $inject3 = "@file_put_contents($f, $fc);"


   // IoC's for the dumped payload

   $payload0 = "function wp_is_mobile_fix()"

   $payload1 = "$is_wp_mobile = ($_SERVER['HTTP_USER_AGENT'] ==
'wp_is_mobile');"

   $payload2 = "$g = $_COOKIE;"
```

```
    $payload3 = "(count($g) == 8 && $is_wp_mobile) ?"


    $url0 = /https?:\/\/(www\.)?wp\-theme\-connect\.com(\/images\/wp\-
theme\.jpg)?/


condition:


    all of ( $inject* )

    or all of ( $payload* )

    or $url0

}
```

Solución:

Recomendamos actualizar inmediatamente los temas o complementos instalados que se encuentren afectados por esta vulnerabilidad a una versión segura indicada en WordPress.org tanto para plugins como para temas. Así también, modificar las contraseñas de los usuarios al wp-admin y a la base de datos.

De forma alternativa recomendamos desinstalar la versión antigua y reinstalar una versión limpia desde la tienda de WordPress.

Información adicional:

- https://thehackernews.com/2022/01/hackers-planted-secret-backdoor-in.html
- https://jetpack.com/2022/01/18/backdoor-found-in-themes-and-plugins-from-accesspress-themes/
- https://blog.segu-info.com.ar/2022/01/backdoor-en-themes-y-plugins-permiten.html
- https://getdigitaltech.com/hackers-planted-secret-backdoor-in-dozens-of-wordpress-plugins-and-themes/