Sistemas de administración de cotenido (CMS)

Capítulo destinado a la solución/mitigación de vulnerabilidades en sistemas de administración de contenidos: wordpress, joomla, drupla y otros.

- Exposición del archivo XMLRPC

Exposición del archivo XMLRPC

En su forma más simple, XML-RPC (llamada a procedimiento remoto) se creó para la comunicación entre plataformas. Este protocolo solía realizar llamadas a procedimientos utilizando HTTP como transporte y XML como codificador. El cliente realiza estas llamadas enviando una solicitud HTTP al servidor y recibe la respuesta HTTP a cambio. XML-RPC invoca funciones a través de una solicitud HTTP y luego estas funciones realizan algunas acciones y envían respuestas codificadas a cambio.

Con el archivo xmlrpc.php habilitado, un actor malintencionado, puede aprovechar las llamadas a procedimeitos remotos (RPC) e invocan funciones para obtener los datos que desean. En la mayoría de los sitios de WordPress, el xmlrpc.php es facilmente rastreable, y con solo enviar datos XML arbitrarios, pueden lograr a controlar el sitio para ejecutar código que han preparado para ejecutar un determinado tipo de ataque.

Solución a la exposición de xmlrpc.php

Puede hacer esto simplemente agregando el bloque de código dentro de su .htaccess. Asegúrese de hacer esto antes de las .htaccess rules que nunca cambian agregadas por WordPress.

```
<Files xmlrpc.php>
order allow,deny
deny from all
</Files>
```

Esto deshabilitará el xmlrpc.php archivo para cada aplicación o servicio que lo use. Puede incluir en la lista blanca una determinada dirección IP en caso de que aún desee acceder a su sitio de WordPress a través de XMLRPC. Para eso, necesitas agregar el siguiente comando:

```
<Files xmlrpc.php>
<RequireAny>
Require ip 1.1.1.2
Require ip 2001:db8::/32
</RequireAny>
</Files>
```