BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-16
Fecha de publicación: 12/06/2024
Tema: Vulnerabilidad RCE en PHP CGI sobre sistemas Windows.
Traffic Light Protocol (TLP): White

Producto(s) afectado:

La vulnerabilidad CVE-2024-4577 afecta a todas las versiones de PHP instaladas en el sistema operativo Windows:

- PHP 8.3 < 8.3.8
- PHP 8.2 < 8.2.20
- PHP 8.1 < 8.1.29

Las ramas de PHP 8.0, PHP 7 y PHP 5 están en EOL y ya no reciben mantenimiento.

Descripción

El 6 de junio del 2024, el equipo de seguridad DEVCORE alertó sobre el descubrimiento una falla de seguridad en el lenguaje de programación PHP específicamente en instalaciones sobre Windows. Dicha vulnerabilidad fue denominada como CVE-2024-4577, con una puntuación de severidad de 9.8 (Critica).

En las versiones de PHP listadas, cuando se usa Apache y PHP-CGI en Windows, si el sistema está configurado para usar ciertas páginas de códigos, Windows puede utilizar el comportamiento "Mejor ajuste" ("Best-Fit") para reemplazar caracteres en la línea de comando proporcionada a las funciones de la API de Win32. El módulo PHP CGI puede malinterpretar esos caracteres como opciones de PHP, lo que puede permitir a un actor malicioso pasar opciones al binario PHP que se está ejecutando y, por lo tanto, revelar el código fuente de los scripts, ejecutar código PHP arbitrario en el servidor (RCE), etc.

Existen dos escenarios de configuración vulnerables:

1. Ejecutar PHP en modo CGI

Al configurar la Directive Action para asignar las solicitudes HTTP correspondientes a un binario ejecutable PHP-CGI en el servidor HTTP Apache, esta vulnerabilidad se puede explotar directamente. Las configuraciones comunes que son afectadas incluyen:

Configuración A

```
AddHandler cgi-script .php
Action cgi-script "/cgi-bin/php-cgi.exe"
```

Configuración B

```
<FilesMatch "\.php$">
    SetHandler application/x-httpd-php-cgi
</FilesMatch>
Action application/x-httpd-php-cgi "/php-cgi/php-cgi.exe"
```

2. Exponer el binario PHP – Configuración predeterminada en XAMPP

Si el PHP no está configurado en el modo CGI, esta vulnerabilidad también se ve afectada por la simple exposición del binario ejecutable de PHP en el directorio CGI. Los escenarios comunes incluyen, entre otros:

1. Copiando cualquiera de los ejecutables php.exe o php-cgi.exe al directorio /cgi-bin/.
2. Exponer el directorio PHP mediante la directiva ScriptAlias, como, por ejemplo:

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

Es importante señalar que el segundo escenario es la configuración predeterminada de XAMPP para Windows , por lo que todas las versiones de las instalaciones de XAMPP en Windows son vulnerables de forma predeterminada hasta el momento de la publicación de este boletín. No se recomienda utilizar XAMPP de licencia gratuita en servidores en producción, el mismo equipo de XAMPP hace esta aclaración.

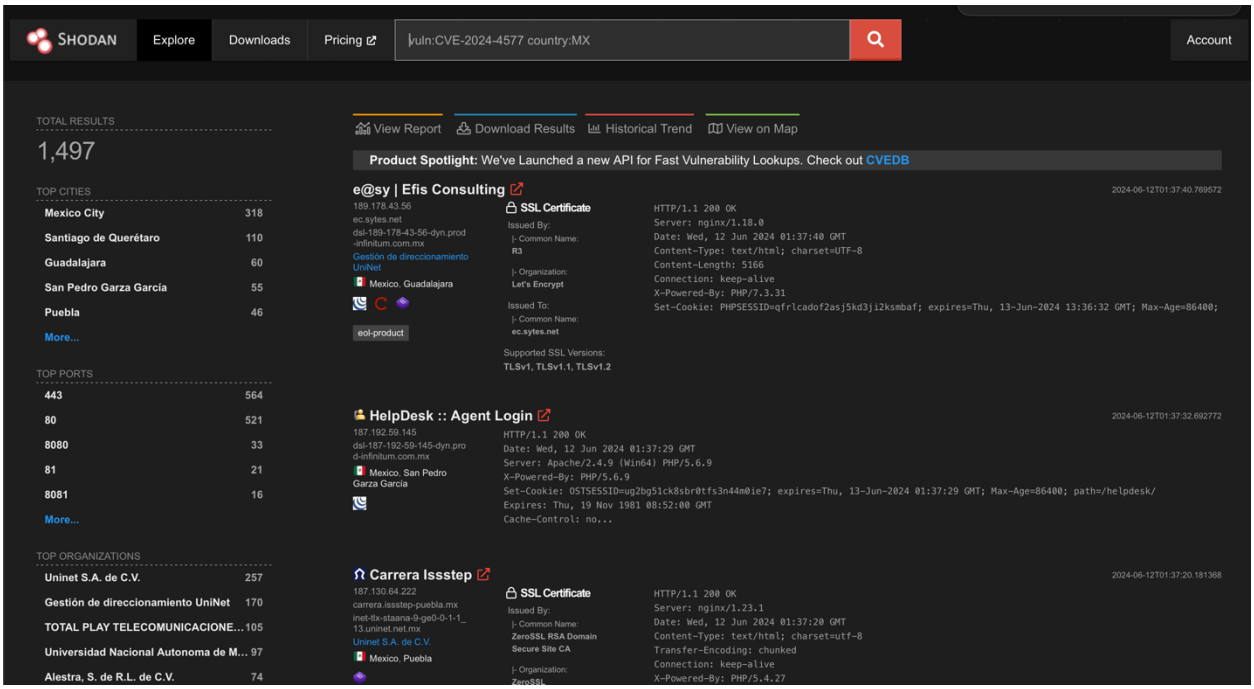
Is XAMPP production ready?

XAMPP is not meant for production use but only for development environments. XAMPP is configured to be open as possible to allow the developer anything he/she wants. For development environments, this is great but in a production environment, it could be fatal.

https://www.apachefriends.org/faq_windows.html

Recientemente se hicieron públicos varios exploits y PoC de esta vulnerabilidad, lo que aumenta por mucho la probabilidad de explotación de esta vulnerabilidad. Tambien, ya existen reportes de Bandas de Ransomware explotando estas vulnerabilidad en sus campañas (como “TellYouThePass”).

En el sitio Shodan se puede visualizar que existen alrededor de 1456 dispositivos vulnerables solo en México.



Impacto

Un actor malintencionado que pueda estar internamente en la red podría aprovechar esta vulnerabilidad para borrar parcial o totalmente las copias de seguridad, con lo que no se podría regresar a un respaldo para recuperar el funcionamiento.

Mitigación

Para los sistemas que no se pueden actualizar, se pueden utilizar las siguientes instrucciones para mitigar temporalmente la vulnerabilidad:

- Para usuarios que no pueden actualizar PHP, las siguientes reglas de reescritura se pueden utilizar para bloquear ataques. Tenga en cuenta que estas reglas son solo una mitigación temporal para las configuraciones regionales de chino tradicional, chino simplificado y japonés ..

```
RewriteEngine On
RewriteCond %{QUERY_STRING} ^%ad [NC]
RewriteRule .? - [F,L]
```

- Para usuarios que usan XAMPP para Windows, cuyo equipo de desarrollo aún no ha publicado los archivos de actualización correspondientes para esta vulnerabilidad al momento de escribir este boletin. Si confirma que no necesita la función PHP CGI, puede evitar la exposición a la vulnerabilidad modificando la siguiente configuración del servidor HTTP Apache: `C:/xampp/apache/conf/extra/httpd-xampp.conf`

Dentro del archivo, comentar la línea correspondiente a:

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

Sin embargo, dado que PHP CGI es una arquitectura obsoleta, se recomienda evaluar la posibilidad de migrar a una arquitectura más segura como Mod-PHP, FastCGI o PHP-FPM.

Solución

Se recomienda a todos los usuarios que actualicen a las últimas versiones de PHP 8.3.8 , 8.2.20 y 8.1.29. A continuación, se encuentra el enlace de descarga oficial:

https://www.php.net/downloads

Información adicional:

- https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/
- https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/
- https://x.com/Shadowserver/status/1799053497490698548
- https://censys.com/cve-2024-4577/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com