Una vulnerabilidad revelada recientemente podría permitir que piratas informáticos controlen remotamente servidores NGINX con la función PHP-FPM habilitada.

La vulnerabilidad, rastreada como CVE-2019-11043, afecta a los sitios web con algunas configuraciones de PHP-FPM, que según los informes, no es infrecuente en la naturaleza y podría explotarse fácilmente como una vulnerabilidad de prueba de concepto PoC.

PHP-FPM es una implementación alternativa de PHP FastCGI que ofrece un procesamiento avanzado y altamente eficiente para scripts escritos en lenguaje PHP.

La vulnerabilidad principal es un problema de corrupción de memoria de flujo interior *«env_path_info»* en el módulo PHP-FPM, y encadenarlo junto con otros problemas podría permitir a los atacantes ejecutar de forma remota código arbitrario en los servidores vulnerables.

Andrew Danau, investigador de seguridad de Wallarm, descubrió la vulnerabilidad al buscar bugs en una competencia de Capture The Flag, que luego fue armada por dos de sus colegas investigadores, Omar Ganiev y Emil Lerner, para desarrollar un exploit de ejecución de código remoto totalmente funcional.

Aunque el exploit PoC lanzado al público está diseñado para apuntar específicamente a servidores vulnerables que ejecutan versiones de PHP 7+, el error de desboramiento PHP-FPM también afecta a versiones anteriores de PHP y podría ser armado de una forma diferente.

Los sitios web son vulnerables en caso de cumplir con lo siguiente:

- NGINX está configurado para reenviar solicitudes de páginas PHP al procesador PHP-FMP
- La directiva fastcgi_split_path_info está presente en la configuración e incluye una expresión regular que comienza con un símbolo ‘^’ y termina con un símbolo ‘$’
- La variables PATH_INFO se define con la directiva fastcgi_param

- No hay comprobaciones como try_files $uri=404 o if (-f $uri) para determinar si un archivo existe o no

Esta configuración vulnerable de NGINX y PHP-FPM es como el siguiente ejemplo:

La directiva fastcgi_split_path_info se utiliza para dividir la URL de las páginas web PHP en dos partes, el valor de un motor PHP-FPM de ayuda para aprender el nombre del script y el otro contiene su información de ruta.

Funcionamiento del exploit PoC RCE para PHP FPM

Según los investigadores, la expresión regular de muestra, que define la directiva fastcgi_split_path_info, puede manipularse utilizando el caracter de nueva línea de forma que la función de división eventualmente establezca la información de ruta como vacía o NULL.

Debido que existe un puntero aritmético en el código FPM que asume incorrectamente que env_path_info tiene un prefijo igual a la ruta del script php sin verificar realmente la existencia del archivo en el servidor, el hacker puede explotar el problema para sobrescribir los datos en la memoria al solicitar URL especialmente diseñadas de los sitios web específicos.

Los investigadores de PoC exploit [1,2], lanzaron cadenas juntas con estos dos problemas para manipular la memoria y agregar valores personalizados de php.ini, como se muestra en la captura de pantalla, en el archivo de configuración PHP-FPM de un servidor de destino, que finalmente, permite a los atacantes ejecutar código arbitrario utilizando un shell web.

> *«Utilizando una longitud cuidadosamente seleccionada de la ruta URL y la cadena*

> *de consulta, un atacante puede hacer que path_info apunte con precisión al primer byte de la estructura _fcgi_data_seg. Al poner cero en él, se mueve el campo `char*pos` hacia atrás, y luego de FCGI_PUTENV sobrescribe algunos datos (incluyendo otras variables cgi rápidas) con la ruta del script»*, dijeron los investigadores en un informe enviado a PHP Project.
>
> *«Utilizando esta técnica, se puede crear una variables falsa PHP_VALUE fcgi y luego utilizar una cadena de valores de configuración cuidadosamente seleccionados para obtener la ejecución del código».*

PHP lanza actualizaciones para corregir la falla de FPM

La lista de condiciones previas para una explotación exitosa, es es poco frecuente ya que algunos de los proveedores de alojamiento web están utilizando las configuraciones vulnerables y están disponibles en Internet como parte de muchos tutoriales de PHP FPM.

Nextcloud, uno de los proveedores de alojamiento web afectados, lanzó ayer un aviso advirtiendo a sus usuarios que *«la configuración predeterminada de Nextcloud NGINX también es vulnerable a este ataque»*, y recomendó a los administradores del sistema que tomen medidas inmediatas.

Ayer se lanzó un parche para esta vulnerabilidad, casi un mes después de que los investigadores lo informaran al equipo de desarrolladores de PHP.

Debido a que el exploit PoC ya está disponible y el parche fue lanzado ayer, es probable que los piratas informáticos ya hayan comenzado a escanear por Internet para buscar sitios web vulnerables.

Debido a esto, es recomendable que los usuarios actualizan PHP a las últimas versiones 7.3.11 y 7.2.24.