Vulnerability Reports de Nmap

CVE-2024-40725

Una corrección parcial de CVE-2024-39884 en el núcleo de Apache HTTP Server 2.4.61 ignora el uso de la configuración heredada de los controladores basada en el tipo de contenido. "AddType" y configuraciones similares, en algunas circunstancias en las que se solicitan archivos de forma indirecta, dan como resultado la divulgación del código fuente de contenido local. Por ejemplo, los scripts PHP pueden ser entregados en lugar de ser interpretados. Se recomienda a los usuarios que actualicen a la versión 2.4.62, que soluciona este problema.

- Afectado desde **el 2.4.60** hasta **el 2.4.61**

Descripción extendida

Los recursos como archivos y directorios pueden quedar expuestos inadvertidamente a través de mecanismos como permisos inseguros o cuando un programa opera accidentalmente sobre el objeto equivocado. Por ejemplo, un programa puede tener la intención de que los archivos privados solo se puedan proporcionar a un usuario específico. Esto define efectivamente una esfera de control que tiene como objetivo evitar que los atacantes accedan a estos archivos privados. Si los permisos de los archivos son inseguros, otras partes que no sean el usuario podrán acceder a esos archivos.

Una esfera de control independiente podría exigir que el usuario solo pueda acceder a los archivos privados, pero no a ningún otro archivo del sistema. Si el programa no garantiza que el usuario solo solicite archivos privados, es posible que pueda acceder a otros archivos del sistema.

En cualquier caso, el resultado final es que un recurso ha sido expuesto a la parte equivocada.

- **Impacto técnico:** *Leer datos de la aplicación; Modificar datos de la aplicación; Otros*