Apache corrigió recientemente múltiples vulnerabilidades en su software de servidor web, que podrían permitir la ejecución de código arbitrario, y en escenarios específicos, causar un bloqueo y denegación de servicio.

Las vulnerabilidades, rastreadas como CVE-2020-9490, CVE-2020-11984 y CVE-2020-11993, fueron descubiertas por Felix Wilhelm de Google Project Zero, y desde entonces han sido abordadas por la Fundación Apache en la última versión del software (2.4.46).

La primera vulnerablidad implica ejecución remota de código, debido a un desbordamiento de búfer con el módulo *«mod_uwsgi»* (CVE-2020-11984), lo que potencialmente puede permitir que un atacante vea, cambie o elimine datos confidenciales según los privilegios asociados con una aplicación que se ejecuta en el servidor.

> *«Una solicitud maliciosa puede resultar en la divulgación de información o ejecución remota de código para un archivo existente en el servidor que se ejecuta en un entorno de proceso malicioso»,* dijo Apache.

El segundo defecto (CVE-2020-11993), se refiere a una vulnerabilidad que se activa cuando la depuración está habilitada en el módulo *«mod_http2».*

CVE-2020-9490, el más grave de los tres problemas, también reside en el módulo HTTP/2, y utiliza un encabezado *«Cache-Digest»* especialmente diseñado, para provocar una corrupción de la memoria que provoque un bloqueo y denegación de servicio.

Cache Digest es parte de una función de optimización web ahora abandonada, que tiene como objetivo abordar un problema con los empujes del servidor, lo que permite que un servidor envíe respuestas de forma preventiva a un cliente antes de tiempo, permitiendo que los clientes informen al servidor de sus contenidos recién almacenados en caché para que no se desperdicie ancho de banda enviando recursos que ya existen en la caché del cliente.

Por lo tanto, al inyectar un valor especialmente diseñado en el encabezado «Cache-Digest»

en una solicitud HTTP/2, se produciría un bloqueo cuando el servidor envía un paquete PUSH utilizando el encabezado. En los servidores sin parches, este problema se puede resolver desactivando la función de inserción del servidor HTTP/2.

Aunque hasta el momento no se han encontrado informes de explotación en la naturaleza, los parches deben aplicarse lo más rápido posible.