Facebook corrigió fallas de “divulgación de memoria con imágenes JPEG” en servidores HHVM

Autor: I. Stepanenko

Fecha: Saturday 21st of September 2019 05:26:43 AM

Facebook solucionó dos vulnerabilidades graves en su aplicación de servidor que podrían haber permitido a los atacantes remotos obtener información confidencial sin autorización o causar una denegación de servicio simplemente cargando un archivo de imagen JPEG creada de forma maliciosa.

Las vulnerabilidades residen en HHVM (HipHop Virtual Machine), una máquina virtual de código abierto de alto rendimiento desarrollada por Facebook para ejecutar programas escritos en PHP y lenguajes de programación.

HHVM utiliza un enfoque de compilación justo a tiempo (JIT) para poder obtener un rendimiento superior de código hack y PHP mientras mantiene la flexibilidad de desarrollo que proporciona el lenguaje PHP.

Debido a que la aplicación del servidor HHVM afectada es de código abierto y gratuita, los dos problemas también pueden afectar a otros sitios web que utilizan HHVM, incluyendo Wikipedia, Box y especialmente lo que permiten a sus usuarios cargar imágenes en el servidor.

Ambas vulnerabilidades, que se muestran a continuación, residen debido a un posible desbordamiento de memoria de la extensión GD de HHVM cuando se pasa una entrada JPEG no construida especialmente, lo que lleva a una lectura fuera de los límites, una falla que permite que un programa con formato incorrecto lea datos desde fuera de los límites de la memoria asignada.

CVE-2019-11925: Se producen problemas de verificación de limites insuficientes al procesar el marcador de bloque JPEG APP12 en la extensión GD, lo que permite a los atacantes potenciales acceder a la memoria fuera de los límites por medio de una entrada JPEG inválida creada con fines malintencionados.

CVE-2019-11926: Se producen problemas de verificación de límites insuficientes al procesar marcadores M_SOFx de encabezados JPEG en la extensión GD, lo que permite a los atacantes potenciales acceder a la memoria fuera de los límites por medio de una entrada JPEG inválida creada con fines maliciosos.

Las dos vulnerabilidades afectar a todas las versiones de HHVM compatibles anteriores a 3.30.9, todas las versiones entre HHVM 4.0.0 y 4.8.3, todas las versiones entre HHVM 4.9.0 y 4.15.2, y las versiones de HHVM 4.16.0, 4.16.3, 4.17.0 a 4.17.2, 4.18.0 a 4.18.1, 4.19.0, 4.20.0 a 4.20.1.

El equipo de HHVM abordó las vulnerabilidades con el lanzamiento de las versiones de HHVM 4.21.0, 4.20.2, 4.19.1, 4.18.2, 4.16.4, 4.15.3, 4.8.4 y 3.30.10.

Si tu sitio web también utiliza HHVM, es recomendable actualizarlo a la últimas versión del software.