Investigadores de seguridad cibernética de Reason Labs, equipo que trabaja junto con el proveedor de soluciones de seguridad, Reason Cybersecurity, revelaron este jueves una vulnerabilidad en la aplicación Facebook Messenger, para Windows.

La vulnerabilidad, que reside en Messenger versión 460.16, podría permitir a los atacantes aprovechar la aplicación para ejecutar potencialmente archivos maliciosos en un sistema comprometido en un intento por ayudar al malware a obtener acceso persistente.

Reason Labs compartió sus hallazgos con Facebook en abril de 2020, después de lo cual, la compañía de redes sociales corrigió rápidamente la falla con el lanzamiento de una versión actualizada de Facebook Messenger para usuarios de Windows por medio de la tienda de Microsoft.

Según los investigadores, la aplicación vulnerable activa una llamada para cargar Windows PowerShell desde la ruta C:\python27. Esta ruta por lo general se crea al instalar la versión 2.7 de python y no existe comúnmente en la mayoría de las instalaciones de Windows.

Los atacantes pueden secuestrar llamadas que intentan cargar recursos potencialmente inexistentes para la ejecución remota de malware encubiertas. Además, debido a que el directorio objetivo también se encuentra en una ubicación de baja integridad, los programas maliciosos podrían acceder a la ruta sin privilegios de administrador.

Para probar si la vulnerabilidad es explotable, el equipo creó un shell inverso disfrazado de Powershell.exe y lo implementó en el directorio de Python. Después, ejecutaron la aplicación Messenger, que activó la llamada, ejecutando con éxito el shell inverso, lo que demuestra que los actores maliciosos podrían explotar la falla para ataques persistentes.

convencionalmente, los atacantes emplean métodos de persistencia que dependen de claves de registro, tareas programadas, y servicios para mantener el acceso activo a un sistema. Este tipo particular de vulnerabilidad se considera como más complejo de explotar, por lo que solamente verdaderos hackers podrían realizar las tareas determinadas para una

correcta vulneración sin necesidad de códigos de terceros.

Los atacantes deben observar si una aplicación está haciendo una llamada o profundizar en el código binario de una aplicación para encontrar una función que realice la llamada.

La vulnerabilidad ya se corrigió en la versión 480.5, que es la versión más reciente que Reason probó. Los usuarios que ejecuta la versión defectuosa deben actualizar a la última versión.

Aunque no ha habido indicios de que la falla haya sido explotada antes del descubrimiento de Reason, las vulnerabilidades son muy peligrosas.

Los hackers pueden usar las vulnerabilidades para mantener acceso a los dispositivos durante períodos prolongados. Este acceso persistente puede permitir realizar otros ataques como la implantación de ransomware y la filtración de datos.

Lo grupos de amenazas también utilizan métodos persistentes para realizar ataques especializados dirigidos a instituciones financieras, oficinas gubernamentales y otras instalaciones industriales.

Además, la amenaza podría haberse extendido si se hubiera explotado la vulnerabilidad. Facebook Messenger tiene 1,300 millones de usuarios activos al mes. Aunque esta cifra representa a todos los usuarios en todos los dispositivos, muchos acceden al servicio por medio de sus máquinas basadas en Windows.

Esto se vuelve más preocupante al tener en cuenta que las aplicaciones de mensajería están teniendo un significado durante la pandemia de coronavirus. Esto debido a las restricciones de viaje, bloqueos y arreglos forzados de trabajo desde el hogar, los usuarios dependen en gran medida de las aplicaciones de mensajería y las herramientas de videoconferencia para comunicarse y colaborar.

Messenger de Facebook se encuentra entre las aplicaciones más populares. En marzo,

Facebook reportó un aumento del 50 por ciento en mensajería y un aumento del 1000 por ciento en el tiempo en grupo en llamadas con tres o más participantes.