Después de que Adobe lanzara actualizaciones para sus productos, Microsoft lanzó este martes un lote mensual de actualizaciones de seguridad para distintas versiones compatibles de los sistemas operativos Windows y otros de sus productos.

Las actualizaciones de seguridad de este mes incluyen parches para 88 vulnerabilidades, de las que 21 están calificadas como críticas, 66 importantes y una con gravedad moderada.

Todas las actualizaciones de junio de 2019 incluyen parches para Windows, Internet Explorer, Edge, Office, ChakraCore, Skype for Business, Microsoft Lync, Microsoft Exchange Server y Azure.

Cuatro de las vulnerabilidades de seguridad, clasificadas como importantes, podrían permitir a hackers escalar privilegios, fueron parcheadas por Microsoft este mes y se revelaron públicamente. No se encontraron explotaciones activas.

Vulnerabilidad reportada por investigador de Google aún no parcheada

Sin embargo, Mcirosoft no ha podido solucionar un defecto menor en SymCrypt, una biblioteca de funciones criptográficas que actualmente utiliza Windows que, en caso de ser explotada de forma exitosa, podría permitir que los programas maliciosos interrumpan el servicio de cifrado de otros programas.

Esta vulnerabilidad fue reportada a Microsoft por Tavis Ormandy, un investigador de seguridad del proyecto Zero de Google, hace casi 90 días. Ormandy publicó hoy detalles y prueba de concepto de la falla luego de descubrir que Microsoft no tiene ningún plan para solucionar el problema con las actualizaciones de este mes.

> *«He podido construir un certificado X.509 que desencadena el error. Descubrí que incrustar el certificado en un mensaje S/MIME, firma de autenticación, conexión de Schannel y ataques DoS efectivos en distintos Windows Server. Obviamente, una gran cantidad de software que procesa contenido no confiable (como un antivirus)*

> *llama a estas rutinas en datos no confiables, y esto hará que se bloqueen»*, dijo Ormandy.

RCE a través de vulnerabilidades de NTLM

Descubiertas por investigadores de Preemp, dos vulnerabilidades de gravedad importantes (CVE-2019-1040 y CVE-2019-1019), afectan el protocolo de autenticación NTLM de Microsoft, que podría permitir a los atacantes remotos eludir los mecanismos de protección NTLM y volver a habilitar los ataques de Relay NTLM.

Estas fallas se originan a partir de tres fallas lógicas que permiten que los atacantes eviten varias mitigaciones, incluido el Código de Integridad del Mensaje (MIC), la Firma de Sesión SMB y la Protección Mejorada para Autenticación (EPA). Microsoft agregó NTLM para prevenir ataques Relay.

En una explotación exitosa, un atacante de tipo intermediario puede *«ejecutar código malicioso en cualquier máquina Windows o autenticarse en cualquier servidor web que admita la autenticación integrada de Windows (WIA), como Exchange o ADFS».*

Las últimas actualizaciones de Microsoft Windows abordan la vulnerabilidad al fortalecer la protección de NTLM MIC en el lado del servidor.

Otras vulnerabilidades importantes de Microsoft

Estas son otras importantes vulnerabilidades de Microsoft para tener en cuenta:

Vulnerabilidades de Windows Hyper-V RCE y ataques DoS (CVE-2019-0620, CVE-2019-0709, CVE-2019-0722). Microsoft corrigió tres vulnerabilidades críticas de ejecución remota de código en Windows Hyper-V, un software de virtualización nativo que permite a los administradores ejecutar sistemas operativos con máquinas virtuales en Windows.

Según los avisos, estas fallas se originan porque la máquina host no valida de forma correcta

las entradas de un usuario autenticado en un sistema operativo invitado.

Los defectos de Hyper-V RCE permiten que un atacante ejecute códigos malintencionados arbitrarios en el sistema operativo del host simplemente ejecutando una aplicación especialmente diseñada en un sistema operativo invitado.

Además de las fallas de RCE en Hyper-V, Microsoft lanzó parches para tres vulnerabilidades de denegación de servicio (DoS) en el software Hyper-V, que podrían permitir que un atacante con una cuenta privilegiada en un sistema operativo invitado colapsara en el sistema operativo host.

Se recomienda a los usuarios y administradores de sistemas que apliquen los últimos parches de seguridad lo antes posible para evitar que los ciberdelincuentes y los piratas informáticos tomen el control de sus computadoras.

Para instalar las actualizaciones de seguridad más recientes, puedes entrar a Configuración > Actualización y seguridad > Actualización de Windows > Buscar actualizaciones en tu computadora.