Microsoft lanzó el día de ayer sus actualizaciones de software de abril 2019 para abordar un total de 74 vulnerabilidades enumeradas en CVE en sus sistemas operativos Windows y otros productos, 13 de los cuales se han calificado como críticos y el resto como graves.

Estas actualizaciones de seguridad solucionan fallas en el sistema operativo Windows, Internet Explorer, Edge, MS Office y MS Office Services y aplicaciones web, ChakraCore, Exchange Server, .NET Framework y ASP.NET, Skype Empresarial, Azure DevOps Server, Open Enclave SDK, Team Foundation Server y Visual Studio.

Ninguna de las vulnerabilidades tratadas este mes por Microsoft se reveló públicamente en el momento del lanzamiento, dejando las dos fallas de día cero descubiertas recientemente en Internet Explorer y Edge aún abiertos para los piratas informáticos.

Sin embargo, se ha informado que dos nuevas vulnerabilidades de escalada de privilegios, que afectan a todas las versiones compatibles del sistema operativo Windows, han sido explotadas activamente en la naturaleza.

Ambas clasificadas como importantes, las fallas (CVE-2019-0803 y CVE-2019-0859) residen en el componente Win32k del sistema Windows, que podría ser explotada por atacantes para ejecutar código arbitrario en modo kernel en una computadora específica.

El mes pasado, Microsoft parchó dos vulnerabilidades similares en el componente Win32k que también fueron explotadas en ataques dirigidos por varios actores de amenazas, incluidos FruityArmor y SandCat.

Además, Microsoft también lanzó actualizaciones para el parche de 13 vulnerabilidades críticas, y como se esperaba, todas las vulnerabilidades de clasificación crítica conducen a ataques de ejecución remota de código excepto una elevación de privilegios en el servidor de Bloque de mensajes de Windows Server (SMB).

Todas las vulnerabilidades críticas afectan principalmente a varias versiones del sistema operativo Windows 10 y las ediciones Server, y residen en ChakraCore Scripting Engine,

Microsoft XML Core Services, SMB Server, Windows IOleCvt Interface y Windows Graphics Devide Interface (GDI).

Muchas vulnerabilidades calificadas de importancia también conducen a ataques de ejecución remota de código, mientras que otras permiten la elevación de privilegios, la divulgación de información, los scripts entre sitios (XSS), la suplantación de identidad y los ataques de denegación de servicio.

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 seguidad más recientes, puedes acceder a *Configuración > Actualización y seguridad > Actualización de Windows > Buscar actualizaciones o instalar las actualizaciones manualmente.*

Para solucionar problemas de actualización en dispositivos con Windows 10, Microsoft también presentó el mes pasado una medida de seguridad que desinstala automáticamente las actualizaciones de software con errores instaladas en tu sistema si el sistema operativo detecta algún error de inicio.

Por otro lado, Adobe también lanzó actualizaciones de seguridad para corregir 40 vulnerabilidades de seguridad en distintos productos.