Fuente:
tynmagazine

Check Point Research, la división de Inteligencia de Amenazas Check Point Software Technologies Ltd. , identificó cuatro vulnerabilidades de seguridad que afectan a los productos del paquete de Microsoft Office, incluidos Excel y Office en línea. Si se explotan, las vulnerabilidades otorgarían a un atacante la capacidad de ejecutar código en objetivos a través de documentos de Office maliciosos, como Word (.DOCX), Excel (.EXE) y Outlook (.EML). Las vulnerabilidades son el resultado de errores de análisis cometidos en el código heredado que se encuentra en los formatos de archivo Excel95, lo que da a los investigadores razones para creer que las fallas de seguridad han existido durante varios años.

CPR descubrió las vulnerabilidades «fuzzing» MSGraph, un componente que se puede incrustar dentro de los productos de Microsoft Office para mostrar gráficos y tablas. Fuzzing es una técnica de prueba de software automatizada que intenta encontrar errores de software pirateados alimentando aleatoriamente entradas de datos no válidas e inesperadas en un programa de computadora, con el fin de encontrar errores de codificación y lagunas de seguridad. Mediante el uso de la técnica, CPR descubrió funciones vulnerables dentro de MSGraph. Verificaciones de código similares confirmaron que la función vulnerable se usaba comúnmente en múltiples productos diferentes de Microsoft Office, como Excel, Office Online Server y Excel para OSX.

Las vulnerabilidades encontradas se pueden incrustar en la mayoría de los documentos de Office. Por tanto, existen múltiples vectores de ataque que se pueden imaginar. El más simple sería:

1. La víctima descarga un archivo de Excel malicioso (formato XLS). El documento se puede entregar a través de un enlace de descarga o un correo electrónico, pero el atacante no puede obligar a la víctima a descargarlo.

2. La víctima abre el archivo de Excel malicioso.

3. Se activa la vulnerabilidad

Dado que todo el paquete de Office tiene la capacidad de incrustar objetos de Excel, esto amplía el vector de ataque, lo que hace posible ejecutar un ataque de este tipo en casi cualquier software de Office, incluidos Word, Outlook y otros.

Yaniv Balmas, director de investigación cibernética de Check Point Software, declaró: “Las vulnerabilidades encontradas afectan a casi todo el ecosistema de Microsoft Office. Es posible ejecutar un ataque de este tipo en casi cualquier software de Office, incluidos Word, Outlook y otros. Aprendimos que las vulnerabilidades se deben a errores de análisis cometidos en el código heredado. Uno de los principales aprendizajes de

nuestra investigación es que el código heredado sigue siendo un eslabón débil en la cadena de seguridad, especialmente en software complejo como Microsoft Office. A pesar de que encontramos solo cuatro vulnerabilidades en la superficie de ataque en nuestra investigación, nunca se puede decir cuántas vulnerabilidades más como estas todavía están esperando ser encontradas. Insto encarecidamente a los usuarios de Windows a que actualicen su software de inmediato, ya que existen numerosos vectores de ataque posibles por parte de un atacante que activa las vulnerabilidades que encontramos «.

Cómo actualizar su PC con Windows

1. Seleccione el botón Inicio, luego seleccione Configuración> Actualización y seguridad> Actualización de Windows.

2. Si desea buscar actualizaciones manualmente, seleccione Buscar actualizaciones.

3. Seleccione Opciones avanzadas y, a continuación, en Elija cómo se instalan las actualizaciones, seleccione Automático (recomendado).

Disponible en:
https://www.tynmagazine.com/descubren-nuevas-vulnerabilidades-en-microso... [1]

Links
[1] https://www.tynmagazine.com/descubren-nuevas-vulnerabilidades-en-microsoft-office/