Cuatro vulnerabilidades de seguridad que se descubrieron en la suite de Microsoft Office, podrían ser potencialmente abusadas por hackers para entregar código de ataque por medio de documentos de Word y Excel.

> *«Arraigadas a partir de código heredado, las vulnerabilidades podrían haber otorgado a un atacante la capacidad de ejecutar código en objetivos a través de documentos de Office maliciosos, como Word, Excel y Outlook»,* dijeron investigadores de Check Point.

Tres de las cuatro vulnerabilidades, rastreadas como CVE-2021-31174, CVE-2021-31178 y CVE-2021-31179, fueron corregidas por Microsoft como parte de su actualización del martes de parches para mayo de 2021. Para la vulnerabilidad (CVE-2021-31939), el parche se incluirá en la actualización del martes de parches de junio, que será lanzada hoy.

En un escenario hipotético de ataque, los investigadores dijeron que la vulnerabilidad podría desencadenarse con el simple hecho de abrir un archivo de Excel malicioso que se envía por correo electrónico o mediante un enlace de descarga.

Debido a los errores de análisis cometidos en el código heredado en los formatos de archivo de Excel 95, las vulnerabilidades se encontraron al confundir MSGraph («MSGraph.Chart.8»), un componente relativamente poco analizado en el componente de Microsoft Office que está a la par del Editor de Ecuaciones de Microsoft, en términos de superficie de ataque. Equation Editor, una función ya desaparecida en Word, se ha convertido en parte del arsenal de varios actores de amenazas relacionados al menos desde finales de 2018.

> *«Debido a que 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»*, dijeron los investigadores.

Las cuatro vulnerabilidades son:

- CVE-2021-31179: Vulnerabilidad de ejecución remota de código de Microsoft Office
- CVE-2021-31174: Vulnerabilidad de divulgación de información de Microsoft Excel
- CVE-2021-31178: Vulnerabilidad china de divulgación de información de Microsoft Office
- CVE-2021-31939: Vulnerabilidad de uso posterior a la liberación de Microsoft Office

Microsoft, en su aviso para CVE-2021-31179, dijo anteriormente que la explotación de la vulnerabilidad requiere que un usuario abra un archivo especialmente diseñado, agregando que el adversario tendría que engañar a las víctimas para que hagan clic en un enlace que redirige a los usuarios al documento malicioso.

Los detalles técnicos exactos sobre CVE-2021-31939 son limitados, seguramente con el fin de que los usuarios tengan tiempo de instalar las correcciones y evitar que los hackers creen exploits dirigidos a la falla.

> *«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. 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»,* dijo Yaniv Balmas, director de investigación cibernética de Check Point.

Se recomienda a los usuarios de Windows que apliquen los parches lo más pronto posible para mitigar el riesgo y evitar ataques que podrían aprovechas las vulnerabilidades mencionadas.