Microsoft lanzó este martes actualizaciones de seguridad para corregir 115 nuevas vulnerabilidades en distintas versiones del sistema operativo Windows y software relacionado, lo que hace de la edición de marzo de 2020, el martes de parches más grande en la historia de la compañía.

De los 115 errores que abarcan sus distintos productos (Microsoft Windows, Edge, Internet Explorer, Exchanger Server, Office, Azure, Windows Defender y Visual Studio), que recibieron nuevos parches, 26 han sido calificados como críticos, 88 recibieron una gravedad de importancia, y uno es moderado en severidad.

Sin embargo, a diferencia del mes pasado, ninguna de las vulnerabilidades que la compañía parchó este mes aparece como públicamente conocida o bajo ataque activo en el momento del lanzamiento.

Cabe resaltar que el parche resuelve fallas críticas que podrían ser potencialmente explotadas por actores maliciosos para ejecutar código malicioso mediante archivos LNK especialmente diseñados y documentos de texto.

Bajo el título *«Vulnerabilidad de ejecución remota de código LNK»* (CVE-2020-0684), la falla permite a un atacante crear archivos de acceso directo LNK maliciosos que pueden realizar la ejecución de código.

> *«El atacante podría presentar al usuario una unidad extraíble, o recurso compartido remoto, que contenga un archivo .LNK malicioso y un binario malicioso asociado. Cuando el usuario abre esta unidad (o recurso compartido remoto) en el Explorador de Windows o cualquier otra aplicación que analice el archivo .LNK, el binario malicioso ejecutará el código de la elección del atacante en el sistema de destino»,* dijo Microsoft en su aviso.

Otro error, una vulnerabilidad de ejecución remota de código de Microsoft Word (CVE-2020-0852), permite que el malware ejecute código en un sistema simplemente al ver

un archivo de Word especialmente diseñado en el Panel de vista previa con los mismos permisos que el usuario conectado. Microsoft advirtió que el Panel de vista previa de Microsoft Outlook también es un vector de ataque para esta vulnerabilidad.

La compañía también emitió correcciones para vulnerabilidades de ejecución remota de código vinculadas a Internet Explorer (CVE-2020-0833, CVE-2020-0824), el motor de secuencia de comandos Chakra (CVE-2020-0811) y el navegador Edge (CVE-2020-0816).

Otra vulnerabilidad importante es CVE-2020-0765, que afecta al Administrador de Conexión de escritorio remoto (RDCMan), para el cual no existe solución.

> *«Microsoft no planea solucionar esta vulnerabilidad en RDCMan y se ha dejado de usar la aplicación. Microsoft recomienda usar clientes de escritorio remoto compatibles y tener precaución al abrir archivos de configuración de RDCMan (.rdg)»,* dice el aviso.