A unas horas de que Adobe lanzara actualizaciones de seguridad para cinco de sus software, Microsoft emitió sus actualizaciones del Patch Tuesday de febrero de 2020, con parches para abordar 99 nuevas vulnerabilidades.

Según las advertencias, 12 de los problemas totales parcheados por la compañía este mes son de gravedad crítica, y los 87 restantes se enumeraron como importantes.

Cinco de los errores se enumeran como conocidos públicamente en el momento del lanzamiento, de los cuales cuatro son importantes y uno crítico (CVE-2020-0674), que también se encuentra bajo ataques activos.

Microsoft advirtió sobre esta vulnerabilidad de día cero en el navegador Internet Explorer (IE) el mes pasado cuando lanzó un aviso sin lanzar un parche para millones de sus usuarios afectados.

Como se explicó antes, la falla podría permitir que un atacante remoto ejecute código arbitrario en computadoras específicas y tome el control total sobre ellas simplemente al convencer a las víctimas de que abran una página web con fines maliciosos en el navegador vulnerable de Microsoft.

Todas las versiones compatibles de Microsoft Windows también tienen una falla crítica de RCE (CVE-2020-0662), que un atacante con cuenta de usuario de dominio puede explotar para ejecutar código arbitrario en el sistema de destino con permisos elevados.

Remote Desktop Client también cuenta con dos problemas críticos, rastreados como CVE-2020-0681 y CVE-2020-0734, que no son errores corregibles, pero y podrían utilizarse para comprometer sistemas vulnerables cuando se conectan a un servidor malicioso o no confiable.

> *«Para aprovechar esta vulnerabilidad, un atacante necesitaría tener el control de un servidor y luego convencer a un usuario para que se conecte a él. Un atacante no*

> *tendría forma de obligar a un usuario a conectarse al servidor malicioso, necesitaría engañar al usuario para conectarse por medio de ingeniería social, envenenamiento de DNS o utilizar una técnica de Hombre en el Medio (MITM). Un atacante también podría comprometer un servidor legítimo, alojar código arbitrario malicioso en él y esperar a que el usuario se conecte.»*, dice el aviso.

Existe otra vulnerabilidad crítica (CVE-2020-0729), que existe en la forma en que el sistema operativo Microsoft Windows analiza los accesos directos LNK, cuya explotación exitosa podría permitir que un atacante remoto ejecute código arbitrario en el sistema afectado y tome el control total de él.

> *«El atacante podría presentar al usuario una unidad extraíble, o recurso compartido remoto, que contiene un archivo .LNK malicioso y un binario malicioso asociado. Cuando el usuario abre esta unidad en el explorador de Windows o cualquier otra aplicación que analiza el archivo .LNK, el binario malicioso ejecutará el código de la elección del atacante en el sistema de destino»,* dice el aviso.

Además, la mayoría de los otros problemas críticos son fallas de corrupción de memoria en IE, el navegador Edge y el motor de secuencias de comandos Chakra, que de ser explotados, también podría permitir que un atacante remoto no autenticado ejecute código arbitrario en un sistema objetivo en el contexto de el usuario actual.

Cabe mencionar que existe un importante problema de omisión de características de seguridad (CVE-2020-0689), que representa una amenaza significativa para los usuarios conscientes de la seguridad. Según Microsoft, hay una vulnerabilidad en la función de arranque seguro que podría permitir que un atacante la omita y cargue software no confiable en el sistema.

Las últimas actualizaciones también tienen parches para múltiples vulnerabilidades de escalada de privilegios, afectando las versiones del sistema operativo Windows, lo que podría

permitir a los hackers con pocos privilegios ejecutar código arbitrario en modo kernel.