Mmicrosoft lanzó ayer de forma silenciosa, actualizaciones de software fuera de banda para parchear dos vulnerabilidades de alto riesgo, que afectan a cientos de millones de usuarios de las ediciones de Windows 10 y Server.

Cabe mencionar que Microsoft se apresuró a lanzar los parches casi dos semanas antes de las próximas actualizaciones de «Patch Tuesday», programadas para el 14 de julio.

Esto es debido a que ambas vulnerabilidades de seguridad residen en la Biblioteca de códecs de Windows, un vector de ataque fácil para las víctimas de ingeniería social que ejecutan archivos multimedia maliciosos descargados de Internet.

Las dos vulnerabilidades recientemente reveladas y asignadas como CVE-2020-1425 y CVE-2020-1457, son errores de ejecución remota de código, que podrían permitir a un hacker ejecutar código arbitrario y controlar la computadora Windows comprometida.

Según Microsoft, ambas vulnerabilidades de ejecución remota de código residen en la forma en que la biblioteca de códecs de Microsoft Windows maneja los objetos en la memoria.

Sin embargo, la explotación de ambos defectos requiere que el atacante engañe a un usuario que ejecuta el sistema Windows afectado, para que haga clic en un archivo de imagen especialmente diseñado para abrirse con cualquier aplicación que utilice la biblioteca de códecs de Windows.

La vulnerabilidad CVE-2020-1425 es la más crítica, debido a que la explotación exitosa podría permitir que el hacker pueda cosechar datos para comprometer aún más el sistema operativo del usuario afectado.

La segunda vulnerabilidad fue calificada como importante y podría permitir que un atacante ejecute código arbitrario en el sistema afectado.

Aún así, no se ha reportado que ninguna de las dos vulnerabilidades haya sido públicamente conocida o explotada activamente por los hackers hasta el momento del lanzamiento de los

parches por parte de Microsoft.

Según las advertencias, Abdul-Aziz Hariri, de la iniciativa Zero Day de Trend Micro, informó a Facebook sobre las vulnerabilidades que afectan a los siguientes sistemas operativos:

- Windows 10 versión 1709
- Windows 10 versión 1803
- Windows 10 versión 1809
- Windows 10 versión 1903
- Windows 10 versión 1909
- Windows 10 versión 2004
- Windows Server 2019
- Windows Server versión 1803
- Windows Server versión 1903
- Windows Server versión 1909
- Windows Server versión 2004

Debido a que Microsoft no tiene conocimiento de ninguna solución o factor atenuante para las vulnerabilidades, es recomendable que los usuarios de dichos sistemas operativos implementen los nuevos parches inmediatamente.

Sin embargo, Microsoft está implementando las actualizaciones de seguridad fuera de banda por medio de Microsoft Store, por lo que los usuarios recibirán la actualización de forma automática sin tener que realizar acciones adicionales.