Microsoft parcheó el año pasado una vulnerabilidad (CVE-2019-0887) de ataque RDP inverso, en el que un sistema cliente vulnerable podría verse comprometido al acceder de forma remota a un servidor por medio del protocolo de escritorio remoto.

Sin embargo, los investigadores pudieron evitar el parche con el simple hecho de reemplazar las barras diagonales en las rutas. Microsoft reconoció la corrección inadecuada y reparó la falla en su actualización del martes de parches de febrero de 2020, con la vulnerabilidad ahora registrada como CVE-2020-0655.

El último informe compartido por Check Point, reveló que Microsoft abordó el problema agregando una solución alternativa en Windows mientras dejaba la raíz del problema de derivación, una función de API «PathCchCanonicalize» sin cambios.

Aparentemente, la solución funciona bien para el cliente RDP incorporado en los sistemas operativos Windows, pero el parche no es tan infalible como para proteger a otros clientes RDP de terceros contra el mismo ataque que se basa en la función de desinfección vulnerable desarrollada por Microsoft.

> *«Descubrimos que un atacante no solo puede pasar por alto el parche de Microsoft, sino que puede pasar por alto cualquier verificación de canonicalización que se haya realizado de acuerdo con las mejores prácticas de Microsoft»,* dijo Eyal Itkin, investigador de Check Point.

Los ataques transversales de la ruta se producen cuando un programa que acepta un archivo como entrada no puede verificarlo, permitiendo que un atacante almacene el archivo en cualquier ubicación elegida en el sistema de destino, con lo que expone el contenido de los archivos fuera del directorio raíz de la aplicación.

> *«Una computadora remota infectada con malware podría hacerse cargo de cualquier cliente que intente conectarse a ella. Por ejemplo, si un miembro del*

> *personal de TI intentara conectarse a una computadora corporativa remota que estaba infectada por malware, el malware podría atacar la computadora del miembro del personal de TI también»*, dijeron los investigadores.

La vulnerabilidad se dio a conocer el año pasado, y una investigación posterior en agosto descubrió que también afectó la plataforma de virtualización de hardware Hyper-V de Microsoft.

Vulnerabilidad incorrectamente parcheada

Según los investigadores, el parche de julio se puede omitir gracias a un problema encontrado en su función de canonicalización de ruta «*PathCchCanonicalize*«, que se utiliza para desinfectar rutas de archivos, lo que permite a un atacante explotar la sincronización del portapapeles entre un cliente y un servidor para colocar archivos arbitrarios en rutas arbitrarias en la máquina cliente.

Dicho de otro modo, cuando se utiliza la función de redireccionamiento del portapapeles mientras está conectado a un servidor RDP comprometido, el servidor puede usar el portapapeles RDP compartido para enviar archivos a la computadora del cliente y lograr la ejecución remota de código.

Aunque los investigadores de Check Point confirmaron originalmente que *«la solución coincide con nuestras expectativas iniciales»*, parece que hay más de lo que parece: el parche se puede evitar simplemente reemplazando las barras diagonales hacia atrás (por ejemplo, archivo \a\ubicación) en las rutas con barras diagonales (por ejemplo, archivo/a/ubicación), que tradicionalmente actúan como separadores de ruta en sistemas basados en Unix.

> *«Parece que PathCchCanonicalize, la función que se menciona en la guía de mejores prácticas de Windows sobre cómo canonicalizar una ruta hostil, ignoró los*

> *caracteres de barra diagonal. Verificamos este comportamiento mediante la ingeniería inversa de la implementación de Microsoft de la función, al ver que divide el camino a las partes buscando solo '\' e ignorando '/'»,* dijo Itkin.

La compañía de seguridad cibernética afirmó que encontró la falla al intentar examinar el cliente de escritorio remoto de Microsoft para Mac, un cliente RDP que quedó fuera de su análisis inicial el año pasado. Curiosamente, el cliente RDP de macOS en sí mismo no es vulnerable a CVE-2019-0887.

Con la vulnerabilidad principal aún sin rectificar, Check Point advirtió que las implicaciones de una simple derivación a una función de saneamiento de ruta central de Windows representan un grave riesgo para muchos otros productos de software que podrían verse afectados.

> *«Microsoft descuidó corregir la vulnerabilidad en su API oficial, por lo que todos los programas que se escribieron de acuerdo con las mejores prácticas de Microsoft seguirán siendo vulnerables a un ataque Path-Transversal. Queremos que los desarrolladores sean conscientes de esta amenaza para que puedan revisar sus programas y aplicar manualmente un parche en su contra»,* dijo Omri Herscovici, de Check Point.