Dos investigadores de seguridad cibernética publicaron hoy los detalles sobre una vulnerabilidad en el servicio de impresión de Windows, que afecta a todas las versiones de Windows que se remontan a Windows NT 4, lanzadas en 1996.

La vulnerabilidad, bajo el nombre PrintDemon, se encuentra en Windows Print Spooler, el componente principal de Windows responsable de administrar las operaciones de impresión.

El servicio puede enviar datos para imprimirlos a un puerto USB/paralelo para impresoras conectadas físicamente, a un puerto TCP para impresoras que residen en una red local o Internet, o en un archivo local, en el supuesto caso de que el usuario quiera guardar un trabajo de impresión para después.

En un informe publicado hoy, los investigadores de seguridad Alex Ionescu y Yarden Shafir, afirmaron que encontraron un error en este viejo componente que se puede abusar para secuestrar el mecanismo interno de Print Spooler.

El error no se puede usar para entrar en un cliente Windows remotamente por medio de Internet, por lo que no es algo que se pueda explotar para hackear sistemas Windows al azar en Internet.

PrimtDemon es una vulnerabilidad de *«escalada de privilegios locales»* (LPE). Esto significa que una vez que un atacante tiene el punto de apoyo más pequeño dentro de una aplicación o máquina Windows, incluso con privilegios de modo de usuario, el atacante puede ejecutar algo tan simple como un comando PowerShell sin privilegios para obtener privilegios de nivel de administrador en todo el sistema operativo.

Esto es posible debido a cómo se diseñó el servicio de cola de impresión para funcionar, según los investigadores.

Debido a que este es un servicio destinado a estar disponible para cualquier aplicación que desee imprimir un archivo, está disponible para todas las aplicaciones que se ejecutan en un sistema, sin restricciones. El atacante puede crear un trabajo de impresión que se imprime

por ejemplo, en un archivo DLL local utilizado por el sistema operativo u otra aplicación.

El atacante puede iniciar la operación de impresión, bloquear el servicio de cola de impresión intencionalmente y luego dejar que el trabajo se reanude, pero esta vez la operación de impresión se ejecuta con privilegios de SYSTEM, lo que le permite sobrescribir cualquier archivo en cualquier lugar del sistema operativo.

Ionescu dijo en Twitter que la explotación en las versiones actuales del sistema operativo requiere una sola línea de PowerShell. En versiones anteriores de Windows, esto podría necesitar algunos ajustes.

> *«En un sistema sin parche, esto instalará una puerta trasera persistente, que no desaparecerá incluso después de parchear»*, dijo Ionescu.

Parches disponibles

La divulgación se hizo pública debido a que la vulnerabilidad ya cuenta con parches, gracias a las correcciones lanzadas por Microsoft este martes para mayo de 2020.

PrintDemon se identifica con CVE-2020-1048. También informaron sobre esto dos investigadores de SafeBreach de forma independiente.

Ionescu publicó un código de prueba de concepto en GitHub con el propósito de ayudar a los investigadores de seguridad cibernética y administradores de sistemas a investigar la vulnerabilidad y preparar mitigaciones y capacidades de detección.

El mes pasado, Ionescu y Shafir también publicaron los detalles y prueba de conecpto para una vulnerabilidad similar a la que llamaron FaxHell.

FaxHell funciona de forma similar a PrintDemon, pero los investigadores explotaron el

servicio de fax de Windows para sobrescribir y secuestrar archivos locales DLL para instalar shells y puertas traseras en los sistemas Windows.