Un exploit de prueba de concepto (PoC) relacionado con una vulnerabilidad de ejecución remota de código que afecta a Windows Print Spooler y parcheado por Microsoft a inicios del mes, se publicó brevemente en línea antes de ser eliminado.

Identificada como CVE-2021-1675, la vulnerabilidad podría otorgar a los atacantes remotos el control total de los sistemas vulnerables. Print Spooler administra el proceso de impresión en Windows, incluyendo la carga de los controladores de impresora adecuados y la programación del trabajo de impresión, entre otros.

Las vulnerabilidades de Print Spooler son preocupantes, no solo por la gran superficie de ataque, sino también por el hecho de que se ejecuta en el nivel de privilegio más alto y es capaz de cargar de forma dinámica binarios de terceros.

Microsoft abordó la vulnerabilidad como parte de su actualización del martes de parches el 8 de junio de 2021. Sin embargo, casi dos semanas después, la compañía revisó el impacto de la falla de una elevación de privilegios a la ejecución remota de código (RCE) y actualizó el nivel de gravedad de importante a crítico.

> *«El atacante aprovecha la vulnerabilidad accediendo al sistema de destino localmente o de forma remota; o el atacante confía en la interacción del usuario de otra persona para realizar las acciones necesarias para aprovechar la vulnerabilidad»,* dijo Microsoft.

El problema para Microsoft dio un giro cuando la compañía de seguridad china QiAnXin reveló a inicios de esta semana que podía encontrar los *«enfoques correctos»* para aprovechar la vulnerabilidad, demostrando así una explotación exitosa para lograr RCE.

Aunque los investigadores se abstuvieron de compartir detalles técnicos adicionales, la empresa de seguridad cibernética con sede en Hong Kong, Sangfor, publicó un análisis profundo independiente de la misma vulnerabilidad, junto con un código PoC en pleno funcionamiento en GitHub, donde permaneció accesible al público antes de que se

desconectara unas horas más tarde.

> *«Eliminamos el PoC de PrintNightmare. Para mitigar esta vulnerabilidad, actualice Windows a la última versión o desactive el servicio Spooler»,* escribió el investigadores de seguridad de Sangfor, Zhiniang Peng en Twitter.

Se espera que los hallazgos sean presentados en la conferencia Black Hat USA el próximo mes.

Windows Print Spooler ha sido por mucho tiempo una fuente de vulnerabilidades de seguridad, por lo que Microsoft ha solucionado al menos tres problemas, CVE-2020-1048, CVE-2020-1300 y CVE-2020-1337, solo en el último año. Particularmente, también se abusó de una vulnerabilidad en el servicio para obtener acceso remoto y propagar el gusano Stuxnet en 2010 contra las instalaciones nucleares iraníes.