El equipo de Project Zero de Google, hizo públicos los detalles de una vulnerabilidad de seguridad de día cero parcheada incorrectamente en la API de cola de impresión de Windows, que podría ser aprovechada por un mal actor para ejecutar código arbitrario.

Los detalles de la falla sin parchear se revelaron de forma pública después de que Microsoft no la parcheara dentro de los 90 días posteriores a la divulgación responsable el 24 de septiembre.

Originalmente rastreada como CVE-2020-0986, la vulnerabilidad se refiere a un exploit de elevación de privilegios en la API GDI Print/Print Spooler («splwow64.exe»), que fue informado a Microsoft por un usuario anónimo que trabaja con Zero Project Initiative de Trend Micro (ZDI), a finales de diciembre de 2019.

Pero al no tener un parche por unos seis meses, ZDI terminó publicando una alerta pública como día cero el 19 de mayo a inicios de este año, luego de lo cual fue explotado en la naturaleza en una campaña denominada «Operation PowerFall» contra una empresa de Corea del Sur no identificada.

splwow64.exe es un binario del sistema central de Windows que permite que las aplicaciones de 32 bits se conecten con el servicio de cola de impresión de 64 bits en sistemas Windows de 64 bits. Implementa un servidor de llamada a procedimiento local (LPC) que puede ser utilizado por otros procesos para acceder a las funciones de impresión.

La explotación exitosa de la vulnerabilidad podría resultar en que un atacante manipule la memoria del proceso splwow64.exe para lograr la ejecución de código arbitrario en modo kernel, y finalmente, usarlo para instalar programas maliciosos, ver, cambiar o eliminar datos, o crear nuevas cuentas con derechos de usuario completos.

Sin embargo, para eso el adversario primero tendría que iniciar sesión en el sistema de destino en cuestión.

Aunque Microsoft finalmente abordó la deficiencia como parte de su actualización del martes

de parches de junio, los nuevos hallazgos del equipo de seguridad de Google revelan que la falla no se ha corregido completamente.

> *«La vulnerabilidad aún existe, solo el método de explotación tuvo que cambiar»,* dijo Maddie Stone, investigadora de Project Zero de Google.
>
> *«El problema original era una desreferencia de puntero arbitraria que permitía al atacante controlar los punteros src y dest a una memoria. La corrección simplemente cambió los punteros a compensaciones, lo que aún permite el control de los argumentos de la memoria»*, agregó Stone.

Se espera que Microsoft resuelva el problema de elevación de privilegios recientemente reportada, identificada como CVE-2020-17008, el 12 de enero de 2021, debido a *«problemas identificados en las pruebas»* después de comprometer una solución inicial en noviembre.

Stone también compartió un código de explotación de prueba de concepto (PoC) para CVE-2020-17008, basado en un PoC lanzado por Kaspersky para CVE-2020-0986.

> *«Ha habido demasiados casos este año de días cero que se sabe que se explotan activamente y se corrigen de forma incorrecta o incompleta. Cuando los días cero no se corrigen por completo, los atacantes pueden reutilizar su conocimiento de las vulnerabilidades y explotar métodos para desarrollar fácilmente nuevos días cero»,* dijo Stone.