Microsoft compartió este jueves una nueva guía sobre otra vulnerabilidad que afecta al servicio Windows Print Spooler, agregando que está trabajando para corregirla en la siguiente actualización de seguridad.

Rastreada como CVE-2021-34481 con puntuación CVSS de 7.8, la vulnerabilidad se refiere a una falla de escalamiento de privilegios local que podría abusarse para realizar acciones no autorizadas en el sistema. La compañía le dio el crédito al investigador de seguridad Jacob Baines, por descubrir y reportar el error.

> *«Existe una vulnerabilidad de elevación de privilegios cuando el servicio Print Spooler realiza de forma incorrecta operaciones de archivos privilegiados. Un atacante que explote exitosamente esta vulnerabilidad podría ejecutar código arbitrario con privilegios de SISTEMA. Un atacante podría instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas con todos los derechos de usuario»,* dijo Microsoft.

Cabe mencionar que la explotación exitosa de la vulnerabilidad requiere que el atacante tenga la capacidad de ejecutar código en un sistema víctima. En otras palabras, esta vulnerabilidad solo puede aprovecharse localmente para obtener privilegios elevados en un dispositivo.

Como soluciones alternativas, Microsoft recomienda a los usuarios detener y deshabilitar el servicio de cola de impresión para evitar que los agentes malintencionados aprovechen la vulnerabilidad.

El desarrollo se produce unos días después de que la compañía implementara parches para corregir una vulnerabilidad crítica en el mismo componente que reveló que estaba siendo explotado activamente para organizar ataques en la naturaleza.

Apodada como PrintNightmare (CVE-2021-34527), la vulnerabilidad se debe a la falta de verificación de permisos en el administrador de trabajos de impresión que permite la

instalación de controladores de impresión maliciosos para lograr la ejecución remota de código o la escalada de privilegios locales en sistemas vulnerables.

Sin embargo, después se supo que la actualización de seguridad fuera de banda podría omitirse por completo en condiciones específicas para obtener tanto la escalada de privilegios locales como la ejecución remota de código. Desde entonces, Microsoft dijo que las correcciones *«funcionan según lo diseñado y son efectivas contra las conocidas vulnerabilidades de cola de impresión de impresoras y otros informes públicos que se denominan colectivamente como PrintNightmare».*