Los investigadores de seguridad cibernética revelaron detalles sobre un par de vulnerabilidades en Microsoft Windows, una de las cuales, podría explotarse para provocar una denegación de servicio (DoS).

Los exploits, denominados LogCrusher y OverLog por Varonis, apuntan al Protocolo de comunicación remota EventLog (MS-EVEN), que permite el acceso remoto a los registros de eventos.

Mientras que el primero permite que *«cualquier usuario de dominio bloquee de forma remota la aplicación de registro de eventos de cualquier máquina con Windows. OverLog provoca un DoS al llenar el espacio del disco duro de cualquier máquina con Windows en el dominio»,* dijo Dolev Taler.

A OverLog se le asignó el identificador CVE-2022-37981 (puntuación CVSS: 4.3) y Microsoft lo abordó como parte de sus actualizaciones del martes de parches de octubre. LogCrusher, sin embargo, sigue sin resolverse.

> *«El rendimiento puede interrumpirse y/o reducirse, pero el atacante no puede negar el servicio por completo»,* dijo la compañía.

Los problemas, según Varonis, se basan en el hecho de que un atacante puede obtener un identificador para el registro heredado de Internet Explorer, preparando de forma efectiva el escenario para ataques que aprovechan el identificador para bloquear el registro de eventos en la máquina de la víctima e incluso inducir una condición DoS.

Esto se logra combinándolo con otra falla en una función de respaldo de registros (BackupEventLogW) para respaldar repetidamente registros de arbitrarios en una carpeta de escritura en el host de destino hasta que se llene el disco duro.

Desde entonces, Microsoft corrigió la falla de OverLg restringiendo el acceso al registro de eventos de Internet Explorer a los administradores locales, reduciendo así el potencial de uso

indebido.

> *«Aunque esto aborda este conjunto particular de exploits de registro de eventos de Internet Explorer, existe la posibilidad de que otros registros de eventos de aplicaciones accesibles para el usuario se aprovechen de forma similar para los ataques»,* dijo Taler.