Microsoft lanzó el martes correcciones para 74 vulnerabilidades de seguridad, incluyendo una para un error de día cero que está siendo explotado activamente en la naturaleza.

De las 74 vulnerabilidades, siete se califican como críticas, 66 como importantes y una de gravedad baja. Dos de las vulnerabilidades se enumeran como conocidas públicamente en el momento del lanzamiento.

Las vulnerabilidades abarcan 24 de ejecución remota de código (RC), 21 de elevación de privilegios, 17 de divulgación de información, seis de denegación de servicio, entre otras. Las actualizaciones se suman a 36 fallas parcheadas en el navegador web Microsoft Edge basado en Chromium el 28 de abril de 2022.

La principal de las vulnerabilidades corregidas es CVE-2022-26925, con puntaje CVSS de 8.1, una vulnerabilidad de suplantación de identidad que afecta a la Autoridad de Seguridad Local de Windows (LSA), que Microsoft describe como un *«subsistema protegido que autentica e inicia sesión en el sistema local».*

> *«Un atacante no autenticado podría llamar a un método en la interfaz LSARPC y obligar al controlador de dominio a autenticarse ante el atacante usando NTLM. Esta actualización de seguridad detecta intentos de conexión anónimos en LSARPC y los rechaza»*, dijo la compañía.

Cabe mencionar que la calificación de gravedad de la falla se elevaría a 9.8 si se encadenara con ataques de retransmisión NTLM en los Servicios de Certificados de Active Directory (AD CS) como PetitPotam.

> *«Al ser explotado activamente en la naturaleza, este exploit permite que un atacante se autentique como usuario aprobado como parte de un ataque de retransmisión NTLM, lo que permite que los actores de amenazas obtengan acceso a los hashes de los protocolos de autenticación»,* dijo Kev Breen, director de

> investigación de amenazas cibernéticas de Immersive Labs.

Otras dos vulnerabilidades conocidas públicamente son:

- CVE-2022-29972 (puntuación CVSS de 8.2) – Insight Software: Magnitude Simba Amazon REdshift ODBC Driver (también conocido como SynLapse)
- CVE-2022-22713 (puntuación CVSS de 5.6): Vulnerabilidad de denegación de servicio de Windows Hyper-V

Microsoft etiquetó CVE-2022-29972, remediada el 15 de abril, como *«explotación más probable»* en el índice de explotabilidad, por lo que es imperativo que los usuarios afectados apliquen las actualizaciones lo antes posible.

Redmond también corrigió varios errores RCE en el sistema de archivos de red de Windows (CVE-2022-26937), LDAP de Windows (CVE-2022-22012, CVE-2022-29130), gráficos de Windows (CVE-2022-26927), kernel de Windows (CVE-2022-29133), Tiempo de ejecución de llamada a procedimiento remoto (CVE-2022-22019) y Visual Studio Code (CVE-2022-30129).

A Cyber-Kunlun, una compañía de ciberseguridad con sede en Beijing, se le atribuye el informe de 30 de las 74 vulnerabilidades.

CVE-2022-22019 sigue un parche incompleto para tres vulnerabilidades RCE en la biblioteca de tiempo de ejecución de llamada a procedimiento remoto (RPC): CVE-2022-26809, CVE-2022-24492 y CVE-2022-24528, que fueron abordadas por Microsoft en abril de 2022.

> *«Aprovechar la falla permitiría a un atacante remoto no autenticado ejecutar código en la máquina vulnerable con los privilegios del servicio RPC»,* dijo Akamai.

La actualización del martes de parches para mayo de 2022 también se destaca por resolver dos vulnerabilidades de escalada de privilegios (CVE-2022-29104 y CVE-2022-29132), y dos

de divulgación de información (CVE-2022-29114 y CVE-2022-29140) en el componente Print Spooler, que ha representado durante mucho tiempo un objetivo atractivo para los atacantes.