Microsoft lanzó el martes soluciones para corregir 64 nuevas vulnerabilidades de seguridad en su línea de software, incluyendo una vulnerabilidad de día cero que se ha explotado activamente en ataques del mundo real.

De las 64 fallas, cinco se califican como críticas, 57 como importantes, una como moderada y una como baja en gravedad. Los parches se suman a 16 vulnerabilidades que Microsoft abordó en su navegador web Edge basado en Chromium a inicios del mes.

> *«En términos de CVE publicados, este martes de parches puede parecer más ligero en comparación con otros meses»,* dijo Bharat Jogi, director de investigación de vulnerabilidades y amenazas en Qualys.

> *«Sin embargo, este mes alcanzó un hito considerable para el año calendario, ya que MSFT fijó el CVE número 1000 de 2022, probablemente en camino de superar el 2021, que parcheó 1200 CVE en total».*

La vulnerabilidad en cuestión explotada activamente es CVE-2022-37969 (puntuación CVSS: 7.8), una falla de escalada de privilegios que afecta al controlador del sistema de archivos de registro común (CLFS) de Windows, que podría ser aprovechada por un atacante para obtener privilegios de SYSTEM en un sistema comprometido.

> *«Un atacante ya debe tener acceso y la capacidad de ejecutar código en el sistema de destino. Esta técnica no permite la ejecución remota de código en los casos en que el atacante aún no tiene esa capacidad en el sistema de destino»,* dijo Microsoft.

La compañía acreditó a cuatro conjuntos distintos de investigadores de CrowdStrike, DBAPPSecurity, Mandiant y Zscaler por informar la falla, que puede ser una indicación de una

explotación generalizada en la naturaleza, según Greg Wiseman, gerente de producto de Rapid7.

CVE-2022-37969 es también la segunda vulnerabilidad de día cero explotada activamente en el componente CLFS después de CVE-2022-24521 (puntuación CVSS: 7.8), la última de las cuales fue resuelta por Microsoft como parte de sus actualizaciones del martes de parches de abril de 2022.

No está claro aún si CVE-2022-37969 es una omisión de parche para CVE-2022-24521. Otras vulnerabilidades críticas son:

- CVE-2022-34718 (puntuación CVSS: 9.8): Vulnerabilidad de ejecución remota de código TCP/IP de Windows
- CVE-2022-34721 (puntuación CVSS: 9.8): Extensiones del protocolo de intercambio de claves de Internet (IKE) de Windows. Vulnerabilidad de ejecución remota de código
- CVE-2022-34722 (puntuación CVSS: 9.8): Extensiones de protocolo de intercambio de claves de Internet (IKE) de Windows. Vulnerabilidad de ejecución remota de código.
- CVE-2022-34700 (puntuación CVSS: 8.8): Vulnerabilidad de ejecución remota de código de Microsoft Dynamics 265 (local).
- CVE-2022-35805 (puntuación CVSS: 8.8): Vulnerabilidad de ejecución remota de código de Microosft Dynamics 265 (local).

> *«Un atacante no autenticado podría enviar un paquete IP especialmente diseñado a una máquina de destino que ejecuta Windows y tiene IPSec habilitado, lo que podría permitir una explotación de ejecución remota de código»,* dijo Microsoft acerca de CVE-2022-34721 y CVE-2022-34722.

Microsoft también resolvió 15 vulnerabilidades de ejecución remota de código en Microsoft ODBC Driver, Microsoft OLE DB Provider para SQL Server y Microsoft SharePoint Server, además de cinco errores de escalada de privilegios que abarcan Windows Kerberos y Windows Kernel.

La versión de septiembre se destaca además por parchear otra vulnerabilidad de elevación de privilegios en el módulo Print Spooler (CVE-2022-38005, puntaje CVSS: 7.8), que podría abusarse para obtener permisos de nivel de SISTEMA.

Finalmente, en la serie de actualizaciones de seguridad se incluye una solución lanzada por el fabricante ARM para una vulnerabilidad de ejecución especulativa llamada Inyección de historial de rama o Spectre-HBH (CVE-2022-23960) que salió a la luz a inicios de marzo.

> *«Esta clase de vulnerabilidades plantea un gran dolor de cabeza para las organizaciones que intentan mitigarlas, ya que por lo general requieren actualizaciones de los mismos sistemas operativos, firmware y, en algunos casos, una recopilación de aplicaciones y refuerzo. Si un atacante explota exitosamente este tipo de vulnerabilidad, podría obtener acceso a información confidencial»*, dijo Jogi.