Las actualizaciones del martes de parches de Microsoft para abril de 2022, abordaron un total de 128 vulnerabilidades de seguridad que abarcan toda su cartera de productos de software, incluyendo Windows, Defender, Office, Exchange Server, Visual Studio, Print Spooler, entre otros.

10 de las 128 vulnerabilidades corregidas fueron calificadas como críticas, 115 como importantes y tres se calificaron como moderadas, con una de las vulnerabilidades enumeradas como conocidas públicamente y otra bajo ataque activo al momento del lanzamiento de los parches.

Las actualizaciones se suman a otras 26 fallas resueltas por Microsoft en su navegador web Edge basado en Chromium desde inicios del mes.

La vulnerabilidad explotada activamente (CVE-2022-24521, con puntaje CVSS de 7.8) se relaciona con una vulnerabilidad de elevación de privilegios en el Sistema de Archivos de Registro Común (CLFS) de Windows.

A los investigadores de la Agencia de Seguridad Nacional (NSA) y de CrowdStrike, Adam Podlosky y Amir Bazine, se les atribuye haber informado sobre la vulnerabilidad.

La segunda vulnerabilidad de día cero conocida públicamente (CVE-2022-26904, con puntaje CVSS de 7.0) también se refiere a un caso de escalada de privilegios en el Servicio de Perfil de Usuario de Windows, cuya explotación exitosa *«requiere que un atacante gane una condición de carrera».*

Otras fallas críticas que se tienen en cuenta incluyen una serie de vulnerabilidades de ejecución remota de código en RPC Runtime Library (CVE-2022-26809, con puntuación CVSS de 9.8), Sistema de Archivos de Red de Windows (CVE-2022-24491 y CVE-2022-24497, puntuaciones CVSS de 9.8), Servicio de Servidor de Windows (CVE-2022-24541), SMB de Windows (CVE-2022-24500) y Microsoft Dynamics 365 (CVE-2022-23259).

Microsoft también corrigió hasta 18 fallas en el servidor DNS de Windows, una vulnerabilidad

en la divulgación de información y 17 fallas en la ejecución remota de código, todas las cuales fueron reportadas por el investigador de seguridad Yuki Chen. También se corrigieron 15 vulnerabilidades de escalada de privilegios en el componente Windows Print Spooler.

Los parches llegan una semana después de que la compañía anunciara planes para poner a disposición una función llamada AutoPatch en julio de 2022, que permite a las empresas acelerar la aplicación de correcciones de seguridad de forma oportuna al mismo tiempo que enfatiza la escalabilidad y la estabilidad.