Recientemente, Microsoft ha anunciado mejoras sustanciales en la seguridad para sistemas que utilizan Exchange Server 2019.

La compañía ha confirmado oficialmente la próxima incorporación de Windows Extended Protection (EP) en estos servidores, proporcionando una breve actualización sobre este asunto. A partir de la instalación de la Actualización Acumulativa H2 2023 (CU14), la función se activará automáticamente como configuración predeterminada.

¿Qué implica la Actualización Acumulativa H2 2023?

Esta herramienta de Protección Mejorada tiene como objetivo fortalecer la funcionalidad de autenticación de Windows Server, brindando una mayor protección contra ataques de intermediarios (MitM).

> Microsoft expresó: *«Queremos informarles que, a partir de la Actualización Acumulativa H2 2023 (CU14) para Exchange Server 2019, EP se habilitará de forma predeterminada cuando se instale CU14 (u versiones posteriores). Actualmente, Exchange Server 2019 está en Soporte Principal y es la única versión que continúa recibiendo Actualizaciones Acumulativas (CUs)».*

Se ha introducido una nueva opción para que los equipos de TI puedan decidir no activar esta función, según lo establecido por el instalador de CU mediante línea de comandos.

Microsoft ha esbozado su recomendación basada en las actualizaciones de seguridad ya implementadas en los puntos finales.

Atención a todos los usuarios que cuentan con la Actualización de Servicio (SU) de agosto de 2022 o posteriores, y tienen EP habilitado: Instalación simple de CU14: Un requisito para usuarios con la SU de agosto de 2022 o posterior, pero que aún no han habilitado EP. Si te encuentras en la categoría de usuarios que han instalado la Actualización de Servicio de

agosto de 2022 o una versión más reciente, pero aún no han habilitado la función EP, entonces se recomienda encarecidamente la instalación de CU14. Es importante destacar que la configuración predeterminada de esta instalación incluye la función «Habilitar EP».

Aquellos usuarios que actualmente están operando con versiones anteriores de Exchange Server a la Actualización de Seguridad (SU) de agosto de 2022 se les recomienda encarecidamente actualizar sus servidores a la SU más reciente.

En un acontecimiento relevante, el Exchange Server recibió una actualización importante en agosto de 2022 con la introducción de la Protección Extendida. En el pasado, Microsoft había informado a los equipos de TI que ciertas vulnerabilidades requerían la activación de características específicas. Se implementó un script que tiene la capacidad de habilitar o deshabilitar automáticamente EP. Notablemente, este script continúa funcionando eficazmente incluso en puntos finales que han recibido actualizaciones posteriores.

> *«Recomendamos que todos los clientes habiliten EP en su entorno. Si sus servidores están utilizando la SU de agosto de 2022 o una SU más reciente, ya admiten EP. Si tienen servidores más antiguos que la SU de agosto de 2022, se considera que esos servidores siguen siendo vulnerables y deben actualizarse de inmediato»,* expresó Microsoft.

> *«Además, si tienen servidores de Exchange anteriores a la SU de agosto de 2022, romperán la comunicación entre servidores que tengan EP habilitado»,* agregó la empresa.