ALERTA: Vulnerabilidad en Windows 10 otorga derechos de administrador (02/DICIEMBRE/2021)

Se reporta a través de fuentes internacionales una vulnerabilidad de escalamiento de privilegios, enfrentando así un alto riesgo de comprometimiento de sistemas de información basados en Microsoft Windows 10.

Introducción

En octubre de 2020 se detectó la vulnerabilidad CVE 2021-24084 de Microsoft OS. Microsoft tenía planes de parchar esta vulnerabilidad en la actualización de febrero de 2021; sin embargo, el parche no reparó la vulnerabilidad en su totalidad, hasta la presente fecha.

Se han publicado parches no oficiales gratuitos para proteger a los usuarios de Windows 10 versión 1809 y posteriores de esta vulnerabilidad, generando una nueva vulnerabilidad de día cero, que permite la escalada de privilegios local (LPE) sin afectar a versiones de Windows Server.

Vector de ataque: Local

El componente vulnerable se hace evidente al momento de activar la opción de "**Exportar los archivos de registro de administración**" que se encuentra en la opción de cuentas de usuarios de la configuración de Windows; ejecutando una serie de subrutinas en segundo plano, abriendo una brecha de acceso para que el(los) atacante(s), escalen privilegios de usuario local a nivel de administrador, a través de capacidades de lectura / escritura / ejecución. O bien: el atacante aprovecha la vulnerabilidad accediendo al sistema de destino localmente (Por ejemplo, teclado, consola) o de forma remota (Por ejemplo SSH); o, el atacante confía en la interacción del usuario por parte de otra persona para realizar las acciones necesarias para aprovechar la vulnerabilidad (Por ejemplo, engañar a un usuario legítimo para que abra un documento malicioso).

En la *Figura 1* a continuación se observa lo descrito anteriormente.

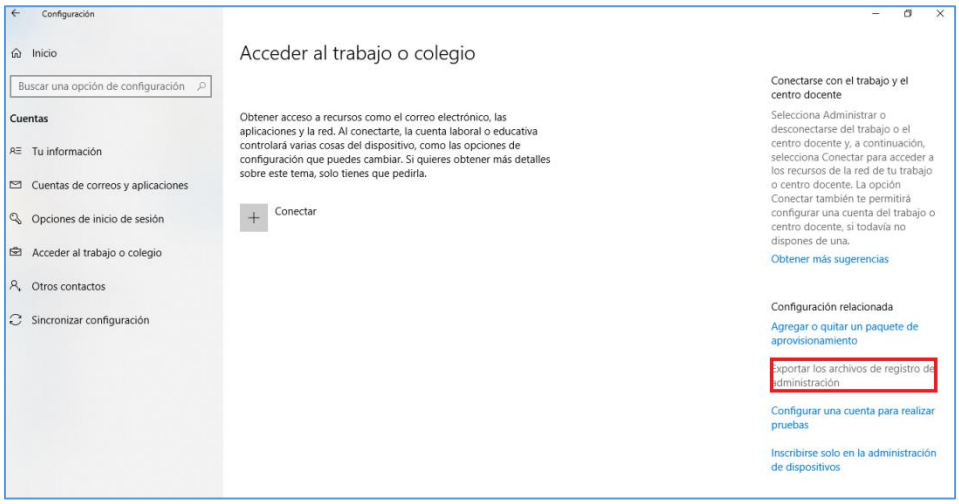

***Figura 1**.- Opción detonante de la vulnerabilidad.*
***Fuente**: Propia.*

Impacto:

Escalamiento de privilegios LPE que genera una pérdida total de confidencialidad, lo que hace que todos los recursos del componente afectado se divulguen al atacante. Alternativamente, se obtiene acceso solo a cierta información restringida, pero la información revelada presenta un impacto directo y serio.

Recomendaciones:

- Utilizar software con licencia legal.
- No activar la función *"Explotar los archivos de registro de administración"*, que se encuentra en la opción de cuentas de usuarios de la configuración de Windows.
- Ejecutar actualizaciones de Microsoft de fuentes oficiales y confirmadas.

Referencias

Ciberseguridad LATAM. (n.d.). Retrieved from https://www.ciberseguridadlatam.com/2021/12/01/el-nuevo-dia-cero-de-windows-10-otorga-derechos-de-administrador-y-recibe-un-parche-no-oficial/

Microsoft. (n.d.). MSRC. Retrieved from https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24084