BOLETÍN DE ALERTA

Boletín Nro.: 2021-17

Fecha de publicación: 23/07/2021

Tema: Vulnerabilidad de elevación de privilegios de Windows 10.

Fecha de actualización: 17/08/2021

Productos afectados:

- Windows: 10 20H2, 10 21H1, 10 2004, 10 1909 y 10 1809

Observación: La vulnerabilidad se introdujo en la versión 1809 de Windows 10 y aunque está presente desde entonces en versiones superiores, sólo estarán afectados los usuarios que hayan actualizado a versiones posteriores de Windows 10 desde la 1809. Es decir, que si se realiza una instalación limpia de Windows 10 20H2, la vulnerabilidad no está activa.

Descripción:

El investigador de seguridad Jonas Lykkegaard ha descubierto una nueva vulnerabilidad que afecta a Windows 10. Se trata de un problema que permite que los archivos del Registro y sus Bases de Datos sean accesibles al grupo "Usuarios" que no tiene privilegios elevados en un dispositivo.

Esto quiere decir que un usuario regular, sin privilegios de Administrador, puede acceder a archivos que contienen información sensible de todas las cuentas del dispositivo. Esto es especialmente problemático en el caso de los archivos del registro asociados con el Administrador de Cuentas de Seguridad (SAM), la base de datos que almacena las contraseñas de los usuarios cifradas.

El fallo puede ser aprovechado por cualquier tipo de usuario para ganar privilegios de Administrador. Esto representa un gran problema ya que cualquier atacante, incluso teniendo privilegios limitados, puede extraer las contraseñas con hash de NTLM de todas las cuentas de un dispositivo y utilizar esos hashes en ataques pass-the-hash para obtener privilegios elevados.

Un ataque pass-the-hash es una técnica en la que el atacante captura el hash de la contraseña en lugar de los caracteres de la misma, y simplemente los usa para autenticarse sin necesidad de tener que descifrar el hash y obtener el password en texto plano.

Microsoft ya ha reconocido la vulnerabilidad identificada como CVE-2021-36934 aún no se ha agregado una calificación de riesgo oficialmente, y la ha descrito como una de elevación de privilegios debido a unas Listas de Control de Acceso (ACLs) demasiado permisivas en múltiples archivos del sistema.

Es importante destacar que el atacante necesita poder ejecutar código en el sistema de la víctima para poder ejecutar esta vulnerabilidad. Microsoft está en proceso de investigación y de momento no han encontrado evidencia de que el fallo esté siendo explotado.

Impacto:

La explotación exitosa de la vulnerabilidad podría permitir a los atacantes remotos no autenticados ejecutar códigos no autorizados/maliciosos como root.

Solución:

Siga las recomendaciones de mitigación ofrecidas por Microsoft e instale los parches de seguridad disponibles.

Después de instalar la actualización de seguridad, debe eliminar manualmente todas las instantáneas de los archivos del sistema, incluida la base de datos SAM, para mitigar por completo esta vulnerabilidad. La simple instalación de esta actualización de seguridad no mitigará por completo esta vulnerabilidad. Consulte KB5005357- Eliminar instantáneas de volumen.

Soluciones alternativas:

- Restringir el acceso al contenido de %windir%\system32\config
    - Abra el símbolo del sistema o Windows PowerShell como administrador.
    - Ejecute este comando:

```
icacls %windir%\system32\config\*.*/inheritance:e
```

- Eliminar instantáneas del Servicio de instantáneas de volumen (VSS)
    - Elimine los puntos de restauración del sistema y los volúmenes de sombra que existían antes de restringir el acceso a %windir%\system32\config.
    - Cree un nuevo punto de restauración del sistema.
- **Impacto de la solución temporal:** Eliminar las instantáneas podría afectar las operaciones de restauración, incluida la capacidad de restaurar datos con aplicaciones de copia de seguridad de terceros.
- **Nota:** Debe restringir el acceso y eliminar las instantáneas para evitar la explotación de esta vulnerabilidad.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934