BOLETÍN DE ALERTA

Boletín Nro.: 2022-04

Fecha de publicación: 17/1/2022

Tema: Vulnerabilidad de ejecución remota de código (RCE) en el protocolo RDP (Remote Desktop Protocol)

Software afectado:

- Microsoft Windows 10 versiones 1809 al 21H2.
- Microsoft Windows 11.
- Microsoft Windows Server versiones 2019 al 2022.

Descripción:

Microsoft ha publicado un parche de seguridad para una vulnerabilidad identificada en el protocolo RDP que permitiría a un atacante (sin privilegios) utilizando la técnica *Man in the Middle* (MitM) a través de un escritorio remoto obtener acceso al sistema de archivos de las máquinas cliente de otros usuarios conectados, visualizar o modificar los datos del portapapeles de otros usuarios conectados y suplantar la identidad de otros usuarios conectados a la máquina por medio de tarjetas inteligentes.

La vulnerabilidad identificada como CVE-2022-21893 de severidad alta, tiene una puntuación de 8.8. Esta se debe a un error de código en el protocolo RDP, el cual permitiría a un atacante utilizar técnicas de ingeniería social (u otra técnica, phishing por ejemplo) con el objetivo de convencer a una víctima de conectarse a un servidor RDP malicioso. Al hacerlo, este podría realizar ejecución remota de código (RCE) en equipo de la víctima.

Para la explotación de la vulnerabilidad se requiere del siguiente escenario:

1. El atacante se conecta a una máquina remota a través de RDP
2. El atacante enumera las canalizaciones (named pipes) abiertas con nombre con el objetivo de encontrar el nombre completo del pipe TSVCPIPE.
3. El atacante crea una instancia de *pipe server* utilizando el mismo nombre a la espera de una nueva conexión
4. Obtenida la nueva conexión el RDS crea su propia instancia de *pipe server* para la sesión, luego un cliente pipe intentara conectarse a la misma.
5. Debido a FIFO, el cliente pipe se conectará a la instancia del *pipe server* del atacante en lugar de a la creada por el servicio RDS.
6. El atacante se conecta como cliente a la instancia real del servidor de *pipe* RDS.
7. En ese momento el atacante posee el control de ambos extremos de la conexión pudiendo actuar como intermediarios, pasando los datos de un lado a otro, visualizándolos y modificándolos (opcionalmente).

Impacto:

La explotación de esta vulnerabilidad permitiría a un atacante podría realizar ejecución remota de código (RCE) en equipo de la víctima.

Detección:
Verificar si el equipo posee a la actualización correspondiente, caso contrario el equipo podría ser vulnerable.

- Microsoft Windows 10 versiones 1809 al 21H2: KB5009555
- Windows 2019: KB5009557
- Windows Server 2022: KB5009555

Solución:

Recomendamos instalar las actualizaciones de seguridad correspondientes al sistema operativo utilizado mediante *Windows Update*, como se indica en la siguiente guía:

- https://support.microsoft.com/en-us/windows/update-windows-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a#WindowsVersion=Windows_10

Adicionalmente recomendamos desactivar los servicios de RDP si no los utiliza, sin embargo, si necesita mantenerlos activos recomendamos:

- No permitir el acceso directo al RDP sino a través de un VPN.
- Usar un Remote Desktop Gateway Server
- Utilizar contraseñas seguras
- Mantener activo Network Level Authentication (NLA)
- Cambiar el puerto del RDP
- Limitar las IP que accedan al RDP

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2022-21893
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21893