Un investigador de seguridad cibernética reveló hoy los detalles de una nueva vulnerabilidad sin parchear en el Protocolo de Escritorio Remoto de Windows (RDP).

Denominada como CVE-2019-9510, la vulnerabilidad reportada permite a los hackers del lado del cliente eludir la pantalla de bloqueo en las sesiones de escritorio remoto.

Descubierta por Joe Tammariello, del Instituto de Ingeniería de Software de la Universidad de Carnegie (SEI), la falla existe cuando la función de escritorio remoto de Windows requiere que los clientes se autentiquen con Autenticación de Nivelde Red (NLA), una función que Microsoft recomendó recientemente como una solución contra el crítico BlueKeep RDP.

Según Will Dormann, una analista de vulnerabilidades en el CERT/CC, es una anomalía de la red desencadena una desconexión RDP temporal mientras un cliente ya estaba conectado al servidor pero la pantalla de inicio de sesión está bloqueada, *«luego de la reconexión, la sesión RDP se restaurará a un estado desbloqueado, independientemente de cómo se dejó el sistema remoto».*

> *«A partir de Windows 10 1803 y Windows Server 2019, el manejo de RDP de Windows de las sesiones RDP basadas en NLA ha cambiado de tal forma que puede causar un comportamiento inesperado con respecto al bloqueo de sesión»,* explicó el investigador.
>
> *«Los sistemas de autenticación de dos factores que se integran con la pantalla de inicio se sesión de Windows, como Duo Security MFA, también se omiten mediante el mecanismo. Cualquier banner de inicio de sesión aplicado por una organización también se omitirá»,* agregó.

Leandro Velasco, del equipo de seguridad de KPN, mostró en el siguiente video lo fácil que es explotar la vulnerabilidad:

El CERT describió el problema de la siguiente forma:

- Un usuario específico se conecta a un sistema Windows 10 o Windows Server 2019 por medio de RDS
- El usuario bloquea la sesión remota y deja el dispositivo cliente sin supervisión
- En ese punto, un atacante con acceso al dispositivo cliente puede interrumpir su conectividad de red y obtener acceso al sistema remoto sin necesidad de brindar credenciales

Esto quiere decir que explotar dicha vulnerabilidad es muy trivial, ya que un atacante solo necesita interrumpir la conectividad de la red de un sistema específico.

Sin embargo, ya que el atacante requiere acceso físico a un sistema tan específico, el escenario en sí limita a la superficie de ataque en mayor medida.

Tammariello notificó a Microsoft sobre la vulnerabilidad el pasado 19 de abril, pero la compañía respondió diciendo que *«el comportamiento no cumplo con los Criterios del Servicio de Seguridad de Microsoft para Windows»,* lo que significa que la compañía no tiene planes para solucionar el problema en corto tiempo.

Aún así, los usuarios pueden protegerse de la vulnerabilidad bloqueando el sistema local en lugar del sistema remoto y desconectado las sesiones de escritorio remoto en lugar de solo bloquearlas.