Cuatro aplicaciones de escritorio remoto VNC de código abierto populares, se encontraron vulnerables a un total de 37 vulnerabilidades de seguridad, muchas de las cuales pasaron desapercibidas durante los últimos 20 años y las más graves podrían permitir que los atacantes remotos comprometan un sistema objetivo.

VNC (Informática de Red Virtual), es un protocolo de uso compartido de escritorio gráfico de código abierto basado en RFB (Remote FrameBuffer), que permite a los usuarios controlar remotamente otra computadora, similar al servicio RDP de Microsoft.

La implementación del sistema VNC incluye un *«componente de servidor»*, que se ejecuta en la computadora que comparte su escritorio, y un *«componente de cliente»,* que se ejecuta en la computadora que accederá al escritorio compartido.

Tomando en cuenta que en la actualidad existen más de 600 mil servidores VNC accesibles remotamente por medio de Internet, y casi el 32% están conectados a sistemas de automatización industrial, los investigadores de seguridad cibernética de Kaspersky auditaron cuatro implementaciones de código abierto ampliamente utilizadas de VNC, que incluyen:

- LibVNC
- UltraVNC
- TightVNC 1.x
- TurboVNC

Después de analizar el software VNC, los investigadores encontraron un total de 37 nuevas vulnerabilidades de corrupción de memoria en software de cliente y servidor, 22 de las cuales, se encontraron en UltraVNC, 10 en LibVNC, 4 en TightVNC y una en TurboVNC.

> *«Todos los errores están relacionados con el uso incorrecto de la memoria. Explotarlos solo conduce a fallos de funcionamiento y denegación de servicio, un resultado relativamente favorable. En casos más graves, los atacantes pueden*

> *obtener acceso no autorizado a la información en el dispositivo o liberar malware en el sistema de la víctima»,* dijo Kaspersky.

Algunas de las vulnerabilidades de seguridad descubiertas también pueden conducir a ataques de ejecución remota de código (RCE), lo que significa que un atacante podría explotar estos defectos para ejecutar código arbitrario en el sistema objetivo y obtener control sobre él.

Debido a que la aplicación del lado del cliente recibe más datos y contiene componentes de decodificación de datos donde los desarrolladores a menudo cometen errores durante la programación, la mayoría de las vulnerabilidades afectan la versión del lado del cliente de este software.

Por otro lado, en el lado del servidor se tiene relativamente una pequeña base de código con casi ninguna funcionalidad compleja, lo que reduce las posibilidades de vulnerabilidades de corrupción de memoria.

Sin embargo, el equipo descubrió algunos errores explotables del lado del servidor, incluyendo una falla de desbordamiento de búfer de pila en el servidor TurboVNC que perite lograr la ejecución remota de código en el servidor.

Pero para explotar esta falla, se requieren las credenciales de autenticación para conectarse al servidor VNC o controlar el cliente antes de establecer la conexión.

Por lo tanto, como protección contra ataques que explotan vulnerabilidades del lado del servidor, se recomienda a los clientes que no se conecten a servidores VNC no confiables o no probados, y los administradores deben proteger sus servidores VNC con una contraseña única y segura.

Kaspersky informó las vulnerabilidades a los desarrolladores afectados, todos estos han emitido parches para sus productos compatibles, excepto TightVNC 1.x que ya no es

compatible con sus creadores. Por lo tanto, se recomienda a los usuarios actualizar a la versión 2.x.