REALVNC® CONNECT INFORME DE SEGURIDAD

Versión 1.5

CONTENIDO

CONTENIDO

INTRODUCCIÓN

La seguridad del cliente es de vital importancia para RealVNC®. Por ello, nuestra estrategia de seguridad está integrada en todos los aspectos de nuestro software RealVNC® Connect. Hemos invertido mucho en nuestra seguridad y estamos muy orgullosos de nuestro exitoso historial. Este documento explica con más detalle nuestra estrategia de seguridad y se divide en cinco temas clave: arquitectura de seguridad, infraestructura en la nube, seguridad del cliente, procedimientos de desarrollo, normas y cumplimiento. Cada uno de ellos se rige por cuatro principios sencillos pero sólidos:

- No tiene por qué confiar en RealVNC para confiar en nuestro software y nuestros servicios.
- No registramos sus sesiones y no podemos descifrar los datos de sesión ni ahora ni en el futuro.
- Cada sesión se trata como si se hiciera en un entorno hostil.
- El propietario del ordenador remoto decide en última instancia quién puede conectarse.

El documento detalla las medidas que tomamos para garantizar que las sesiones de acceso remoto de VNC Connect sean lo más seguras posible. Además de estas estrategias de seguridad, también disponemos de un Centro de Operaciones de Seguridad (SOC) 24x7 y contamos con varias certificaciones de datos, como GDPR e IEC/ISO 270001.

Acceso a dispositivos	Una función integrada en RealVNC Connect que permite el acceso asistido o sin supervisión a los ordenadores que posea o administre con RealVNC Connect instalado. Más información.
Asistencia a la carta (antes denominada Asistencia instantánea)	Una función integrada en RealVNC Connect que permite el acceso asistido bajo demanda a ordenadores que no tienen o no pueden tener instalado RealVNC Connect. Más información.
Visualizador RealVNC	Una aplicación del cliente que le permite controlar un ordenador remoto. Se ejecuta en el ordenador o dispositivo móvil desde el que se desea controlar. En este documento, el visualizador RealVNC también se utiliza para referirse al "dispositivo en el que se ejecuta el visualizador RealVNC"
Servidor RealVNC	Una aplicación del cliente que permite controlar un ordenador remoto. Como parte de su suscripción RealVNC Connect, donde usted tiene: • Para acceder al dispositivo, es necesario instalar previamente el servidor RealVNC (que forma parte de la descarga de RealVNC Connect) y obtener una licencia en los ordenadores remotos. • Asistencia a la carta, a continuación, el servidor RealVNC (en forma de aplicación desechable) se descarga justo a tiempo para conectarse remotamente a ordenadores y no necesita instalarse ni obtener licencia. En este documento, el servidor RealVNC se utiliza para indicar a la aplicación cualquiera de estos 'modos', y además de "el ordenador en el que se ejecuta el servidor RealVNC".
Conexión a la nube	Una sesión de acceso remoto intermediada por los servicios en la nube de RealVNC. Siempre que sea posible, una vez intermediada y asegurada, la sesión se gestiona entre iguales. Si no es posible, los servicios en la nube de RealVNC retransmiten los datos de la sesión.
Conexión directa	Una sesión de acceso remoto que se lleva a cabo totalmente entre iguales, sin ningún tipo de comunicación a través de los servicios en la nube de RealVNC. Solo está disponible con una suscripción Premium o Enterprise.

ARQUITECTURA DE SEGURIDAD

Visión general

En RealVNC, asumimos como premisa fundamental de seguridad que la conexión entre el Visualizador RealVNC y el Servidor RealVNC puede atravesar un entorno hostil, y hemos construido toda nuestra arquitectura de seguridad teniendo esto en cuenta. Como tal, las características y estrategias de seguridad que se describen a continuación se aplican por igual a los métodos de conexión en la nube y directa (TCP).

Al establecer una conexión en la nube, los servicios en la nube de RealVNC sólo intermedian en las conexiones aprobadas y actúan como mecanismo de transporte alternativo para los datos cifrados. No gozan explícitamente de una posición de seguridad privilegiada. La máxima responsabilidad de autorizar el acceso remoto recae exclusivamente en el servidor RealVNC.

Al realizar una conexión directa, el Visualizador RealVNC utiliza una conexión TCP directa con el Servidor RealVNC, sin realizar interacción alguna con los servicios en la nube de RealVNC. Los clientes son autosuficientes y no necesitan acceso a Internet. Una vez más, el Servidor RealVNC es en última instancia el responsable de conceder el acceso remoto autorizado.

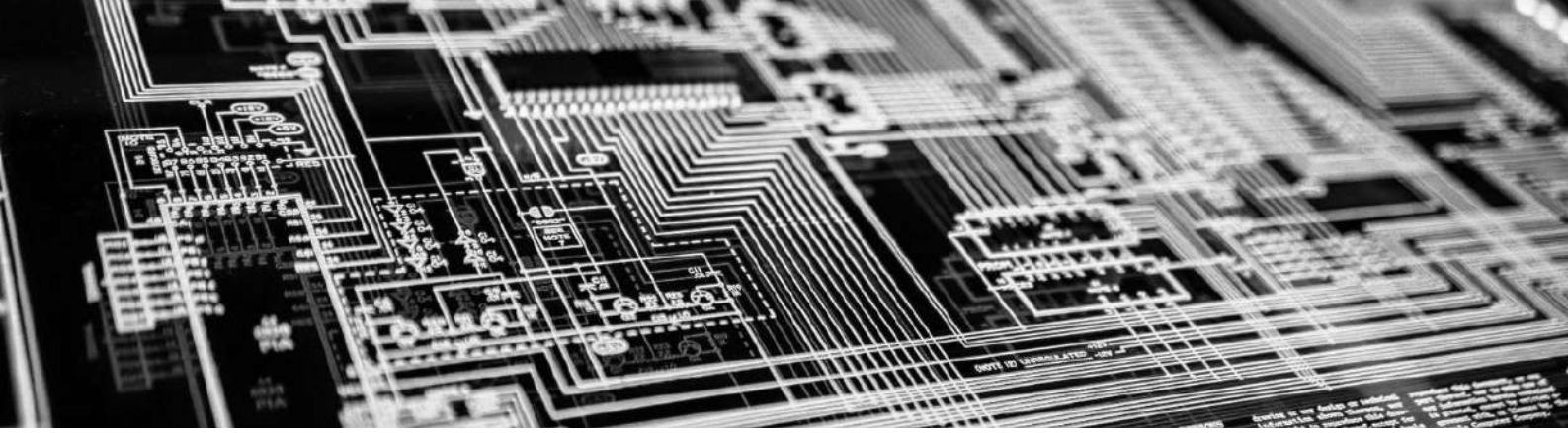
Protocolo Remote Framebuffer (RFB)

La tecnología RealVNC utiliza el Protocolo Remote Framebuffer, un protocolo estándar de Internet creado originalmente por RealVNC como primer protocolo de escritorio remoto. RealVNC continúa manteniéndolo activamente, lanzando la versión 5 de RFB en junio de 2015 que fue diseñada desde cero para soportar la conectividad en la nube. En enero de 2019, se lanzó la versión 6 de RFB añadiendo soporte para UDP, audio y mejorando el rendimiento de la transmisión.

RFB 5 exige el uso de suites de cifrado modernas y utiliza criptografía robusta en todas sus partes. Está simplificada en comparación con TLS, lo que la hace mucho menos propensa a vulnerabilidades de implementación y a errores de configuración. Ofrece un intercambio de claves muy sólido que está diseñado para la conectividad en la nube, mezclando tres fuentes de material clave: el cliente local, el cliente remoto y el procedimiento de autenticación “handshake” en la nube. De este modo, los clientes tienen el control total de las claves de cifrado, lo que impide su manipulación. Puede encontrar un análisis de seguridad detallado de RFB aquí.

Cifrado

RealVNC Connect utiliza el cifrado AES-GCM para garantizar el secreto y la integridad de los datos en tránsito. Todos los tipos de suscripción a RealVNC Connect admiten el cifrado AES de 128-bits, con la opción de aumentarlo a 256-bits. Todo el cifrado es de extremo a extremo, lo que garantiza que nadie pueda leer los datos en tránsito, incluido RealVNC. El intercambio de claves Diffie-Hellman de curva elíptica añade el Secreto Perfecto Hacia Adelante (PFS) al intercambio de claves RSA utilizado para la comprobación de identidades (consulte la sección Comprobación de identidades, más adelante). PFS proporciona un secreto compartido para cada conexión individual que sólo puede recuperarse mientras la conexión está activa, evitando que las claves filtradas se utilicen para descifrar conexiones pasadas o futuras.



Control de identidad

El modelo de comprobación de identidad de RealVNC permite al Visualizador RealVNC saber que se está conectando al ordenador correcto, evitando la suplantación de identidad. Cada cliente se identifica mediante una clave RSA según dos modelos de seguridad diferentes:

- Para las conexiones directas, se emplea un modelo de "Confianza en el primer uso" (TFU). En este caso, el usuario del Visualizador RealVNC debe aprobar manualmente cada clave la primera vez que se realiza una conexión a un nuevo ordenador. El Visualizador RealVNC almacena las claves y se asegura de que no han cambiado en la reconexión. Esto garantiza que nadie ha interceptado la conexión.

- Para las conexiones en la nube, los servicios en la nube de RealVNC verifican automáticamente la identidad, lo que significa que el usuario del Visualizador RealVNC no necesita comprobar la clave manualmente. Sin embargo, con el acceso a dispositivos, no es necesario que los usuarios del Visualizador RealVNC confíen en esta verificación automática de identidad. Los usuarios pueden realizar una comprobación de identidad manual en el momento de la conexión para garantizar que nuestros servicios no han interceptado la conexión.

Al realizar la comprobación manual de identidad, la identidad del Servidor RealVNC se presenta como una frase fácilmente reconocible. De este modo, los usuarios pueden detectar fácilmente los cambios en la clave del Servidor RealVNC, lo que evita la suplantación de identidad. La frase se deriva de la clave RSA del Servidor RealVNC y es una representación legible de la huella digital de la clave.

Proceso de negociación de la nube

La conectividad en la nube permite acceder fácilmente a las máquinas a través de NAT y los Cortafuegos. Para ello, utiliza una conexión saliente a los servicios en la nube de RealVNC desde el Visualizador RealVNC y el Servidor RealVNC. Estos servicios actúan como intermediarios en la conexión, lo que les permite intercambiar direcciones IP para la conectividad entre iguales, y también pueden retransmitir datos en caso de que la conectividad entre iguales no sea posible. Una vez establecida la conexión, se aplica la misma seguridad de RFB, independientemente del mecanismo de transporte. Los clientes siempre asumen que el transporte podría ser hostil, incluso si se transporta a través de nuestros servicios. RealVNC no tiene capacidad para leer o manipular ninguna conexión.

Al evitar el uso de paquetes TCP o UDP entrantes, RealVNC Connect no requiere que se abra ningún puerto en su los Cortafuego. Esto impide el acceso no autenticado a su red desde el exterior.

Negociación de la conectividad entre iguales

Cuando se utiliza la conectividad entre iguales con conexiones en la nube, se emplea el procedimiento estándar de Establecimiento de Conectividad Interactiva (ICE). Esto implica abrir un puerto UDP en cada cliente, realizar el descubrimiento de la dirección IP mediante STUN y, a continuación, enviar paquetes directamente al par. El Servidor RealVNC sólo abre los puertos UDP necesarios cuando se establece una conexión y los asocia a una conexión específica, lo que reduce al mínimo la superficie de ataque.

Esto funciona a un nivel inferior que la RFB, por lo que se utiliza un mecanismo de seguridad independiente para firmar cada paquete UDP, utilizando un secreto por conexión. Así se evitan los ataques contra el puerto UDP y la interceptación de la conexión en un nivel inferior al de los datos RFB. Entre las capas ICE y RFB, se utiliza SCTP para añadir fiabilidad al flujo de datos.

NUBE INDEPENDIENTE Y CREDENCIALES DEL SERVIDOR REALVNC

Acceso a dispositivos

Para controlar un dispositivo remoto de su propiedad o gestionarlo a través de la nube, debe introducir una serie de credenciales de autenticación únicas:

- En primer lugar, para descubrir un equipo, debe haber sido invitado al "equipo" de ese computador. Se puede implementar un control de acceso adicional mediante el uso de Grupos. La capacidad de descubrimiento puede restringirse a usuarios o grupos de usuarios específicos.

- A continuación, debe iniciar sesión en el Visualizador RealVNC utilizando las credenciales de su cuenta RealVNC para ese Equipo.

- Una vez seleccionado un dispositivo, deberá introducir sus credenciales de autenticación. Por defecto, el Servidor RealVNC solicita los datos que se utilizan normalmente para iniciar sesión en ese dispositivo, aunque puede cambiar el esquema de autenticación o aumentar el número de factores si lo desea (consulte la sección Autenticación multifactor para el Servidor RealVNC, más adelante). Las listas de control de acceso configuradas en el Servidor RealVNC (localmente o mediante políticas) determinan quién puede obtener acceso remoto y qué acciones puede realizar si se le concede el acceso.

Asistencia a la carta

Para controlar un dispositivo remoto bajo demanda a través de la nube, tanto usted como el propietario de ese dispositivo debéis cooperar para introducir dos conjuntos de credenciales de autenticación.

- En primer lugar, debe haber sido invitado a un equipo de RealVNC Connect para el que se le haya concedido explícitamente la función de técnico.

- A continuación, debe iniciar sesión en el Visualizador RealVNC utilizando las credenciales de su cuenta RealVNC para ese Equipo y generar un código único de 9 dígitos para la sesión.

- Para conectarse, debe dar el código de 9 dígitos al propietario del dispositivo fuera de banda. Solo cuando el propietario del dispositivo introduzca el código correcto podrá iniciarse la sesión.

Estos pasos garantizan que los dispositivos remotos estén protegidos por múltiples mecanismos de autenticación. Ninguna contraseña controla el acceso remoto.

INFRAESTRUCTURA EN NUBE

El acceso a los datos de los servicios está estrictamente controlado y se concede caso por caso, con la aprobación de la alta dirección de RealVNC. Cada cambio realizado por el equipo se registra con fines de auditoría.

Visión general

Nuestra filosofía para la nube es que ninguna medida de seguridad es primordial. En otras palabras, nuestra seguridad es estratificada; si los servicios en la nube de RealVNC fueran violados, o si un tercero malintencionado obtuviera acceso a las credenciales de su cuenta RealVNC, no hay forma de que ese tercero obtenga acceso remoto a sus ordenadores.

Servicios en la nube de RealVNC

RealVNC Connect inicia y mantiene una conexión a través de la nube utilizando nuestro sistema de servicios en línea, diseñado internamente junto con nuestro equipo de seguridad. Estos se ejecutan en una plataforma de seguridad reforzada.
Estos servicios están protegidos por TLS obligatorio, y todos los puntos finales están debidamente autenticados. Todos los clientes utilizan TLS 1.2 cuando se comunican con los servicios en la nube. Utilizamos limitación de velocidad y distribución geográfica para defendernos de los ataques de denegación de servicio. Como nuestra arquitectura distribuida no tiene nodos maestros, nuestros servicios son de alta disponibilidad. Esto garantiza el mantenimiento del servicio a los clientes durante las actualizaciones y la conmutación por error. Los datos se replican en tiempo real en varios centros de datos, y se guardan copias de seguridad frecuentes de las bases de datos en un almacenamiento cifrado con fines de recuperación.

Operaciones

Nuestro equipo de operaciones técnicas supervisa los servicios en la nube de RealVNC 24 horas al día, 365 días al año. Estos sistemas se parchean con regularidad. Cualquier vulnerabilidad crítica en las dependencias ascendentes se evalúa y parchea fuera de nuestro programa regular de parches. Nuestro Centro de operaciones de seguridad 24x7 supervisa las amenazas y los eventos de seguridad en los sistemas RealVNC y la infraestructura de red.

El acceso a los datos de los servicios está estrictamente controlado y se concede caso por caso, con la aprobación de la alta dirección de RealVNC. Cada cambio realizado por el equipo se registra con fines de auditoría. Los servidores que contienen datos sensibles utilizan la detección de intrusiones basada en host. Si alguien accediera sin autorización, se producirían alertas automáticas. En todos los servidores con acceso a Internet se realiza regularmente un escaneado automatizado de puertos externos. Nuestro equipo de seguridad revisa periódicamente los resultados.

Infraestructura de clave pública

La comunicación dentro del servicio está protegida mediante una infraestructura de clave pública (PKI) cerrada. En el funcionamiento interno de esta PKI se aplican las mejores prácticas del sector y se utilizan los mejores dispositivos de seguridad (incluidos módulos de seguridad de hardware y discos duros cifrados AES de

256-bits). Al controlar la cadena de confianza de extremo a extremo, garantizamos que está estrechamente controlada y no depende de autoridades de certificación raíz de terceros.

Los datos sensibles nunca se almacenan en la nube

El Servidor RealVNC no delega la autenticación en la nube. En su lugar, realiza sus propias comprobaciones de autenticación, lo que significa que no se puede utilizar ninguna infracción de los datos de la nube para obtener acceso a los ordenadores. Tenga en cuenta que, para el acceso a los dispositivos, el Visualizador RealVNC siempre almacena las contraseñas de los ordenadores para aquellos usuarios que deciden guardarlas cómodamente de forma local, y nunca las envía a la nube.

Del mismo modo, la información de pago no se almacena en la nube. En su lugar, se almacena en una cámara acorazada segura propiedad de un proveedor de pagos externo. Su sistema de almacenamiento cumple la normativa PCI DSS.

Las credenciales de su cuenta RealVNC se almacenan de forma segura, utilizando hashes Bcrypt con una sal aleatoria. Si decide eliminar su cuenta RealVNC, sus datos se eliminarán por completo de nuestros servidores.

Portal de gestión de cuentas RealVNC

Nuestro portal en línea puede utilizarse para gestionar su cuenta RealVNC, así como para controlar los usuarios y el dispositivo de su equipo. Muchas de las funciones de seguridad de esta sección se administran a través del portal.

El acceso al propio portal está protegido por TLS obligatorio. Nuestro sitio web ha obtenido la calificación A en la prueba Qualys SSL Labs.

Las credenciales de su cuenta RealVNC se almacenan de forma segura, utilizando hashes Bcrypt con una sal aleatoria. Si decide eliminar su cuenta RealVNC, sus datos se eliminarán por completo de nuestros servidores.

Seguimos todas las mejores prácticas de desarrollo web seguro, incluido el uso de cookies seguras y la protección contra la inyección de contenido y el cross-site scripting (XSS). Para evitar el uso indebido de la sesión, los usuarios que inician sesión se desconectan automáticamente tras un periodo de inactividad.

Gestión de funciones en línea

La gestión de roles en línea para su equipo está integrada en el portal. Actualmente existen cuatro funciones:

- **Usuario.** Puede iniciar sesión en el Visualizador RealVNC y acceder remotamente a los equipos. No pueden gestionar el equipo de ninguna manera.

- **Administrador.** Un usuario que, además, puede invitar a otras personas para compartir el acceso remoto, añadir dispositivos al equipo (acceso a dispositivos) o nombrar técnicos (Asistencia a la Carta).

- **Administrador.** Un Administrador que, además, puede añadir capacidad, renovar suscripciones y gestionar métodos de pago.

- **Propietario.** El propietario puede hacerlo todo, incluso cambiar la dirección de facturación y el número de IVA de todos sus equipos.

Autenticación multifactor para su cuenta RealVNC

Por defecto, su cuenta RealVNC está protegida utilizando el correo electrónico como segundo factor. Cada vez que inicie sesión en línea o en el Visualizador RealVNC desde un nuevo dispositivo en una nueva ubicación, recibirá un correo electrónico solicitándole que confirme la actividad. El correo electrónico registra la hora, la ubicación y el tipo de dispositivo que intenta acceder a su cuenta. Esto garantiza que nadie pueda acceder a su cuenta, aunque descubra o adivine las credenciales de su cuenta RealVNC (dirección de correo electrónico y contraseña).

A continuación, se recuerda el dispositivo, por lo que no se le pedirá que confirme en ese dispositivo de nuevo, ni en ningún otro dispositivo en la ubicación ahora de confianza, a menos que elija explícitamente olvidarlo (véase más adelante).

Puede proteger aún más su cuenta RealVNC activando la verificación en dos pasos en el portal web de RealVNC. Esto significa que cada vez que inicie sesión en línea o en el Visualizador RealVNC se le pedirá que introduzca un token TOTP (un estándar de Internet utilizado por Google Authenticator y aplicaciones similares) además de las credenciales de su cuenta. Efectivamente, TOTP sustituye al correo electrónico como segundo factor, y proporciona un mayor nivel de seguridad al requerir confirmación para cada inicio de sesión.

Autenticación multifactor obligatoria para su equipo

Si dispone de una suscripción Enterprise, los gestores, administradores y propietarios de equipos pueden exigir la verificación en dos pasos para los miembros del equipo (incluidos ellos mismos). Esto significa que todos los miembros de un equipo, cada uno de los cuales tiene su propia cuenta RealVNC, deben activar la verificación en 2 pasos para poder participar en el equipo, y el acceso

A continuación, se recuerda el dispositivo, por lo que no se le pedirá que confirme en ese dispositivo de nuevo, ni en ningún otro dispositivo en la ubicación ahora de confianza, a menos que elija explícitamente olvidarlo

remoto se bloquea hasta que cumplen. Posteriormente, cada miembro del equipo introduce un token TOTP además de las credenciales de su cuenta cada vez que inicia sesión en el visualizador VNC.

Cierre de sesión remoto desde dispositivos recordados

En el portal web de RealVNC, puede cerrar la sesión de forma remota (es decir, olvidarse) de los dispositivos conectados a su cuenta RealVNC. Para los dispositivos conectados al Visualizador RealVNC, esto elimina además cualquier contraseña del Servidor RealVNC almacenada localmente, así como los datos almacenados en caché de su libreta de direcciones. Este sistema de seguridad garantiza que, en caso de robo o extravío del hardware, un tercero malintencionado no podrá acceder a su cuenta RealVNC.

SEGURIDAD DEL CLIENTE

Visión general

RealVNC Connect consta de dos aplicaciones: El Servidor RealVNC y el Visualizador RealVNC. El Visualizador RealVNC se utiliza para obtener acceso remoto a ordenadores que ejecutan el Servidor RealVNC.
El software cliente del Servidor RealVNC es siempre responsable de asegurar el acceso al ordenador. El Servidor RealVNC controla la autenticación y autorización del Visualizador RealVNC y concede el acceso. Por el contrario, algunas soluciones utilizan un dispositivo de puerta de enlace o mecanismos de control en la nube para verificar y conceder el acceso a una sesión remota. RealVNC nunca difiere el control de acceso a un dispositivo o a la nube. Dado que el Servidor RealVNC mantiene el control en todo momento, se reduce la superficie de ataque global.

Registro de auditoría

Acceso a dispositivos

El Servidor RealVNC escribe una entrada de auditoría en el registro del sistema de cada plataforma por cada conexión realizada. Esto recopila una amplia gama de información de conexión y puede almacenarse localmente o en un controlador de dominio. Estos registros se pueden utilizar para inspeccionar y auditar conexiones individuales, y resultan extremadamente útiles para respaldar el cumplimiento corporativo y los requisitos de gobierno normativo.

Asistencia a la carta

Los servicios en la nube de RealVNC almacenan un registro de cada sesión de asistencia y lo ponen a su disposición en la página Sesiones del portal en línea. Si está disponible en su suscripción a RealVNC, puede profundizar en una sesión individual en línea y examinar un registro de actividad detallado, que consta de transcripciones de chat, detalles de archivos transferidos, solicitudes de elevación y operaciones de reinicio. Las transcripciones de chat se cifran en reposo en los servidores de RealVNC.

Listas negras (sólo acceso de dispositivos)

El Servidor RealVNC dispone de listas negras por IP que impiden que los clientes no autenticados realicen solicitudes de autenticación repetidas. En los sistemas UNIX, la función de lista negra se aplica adicionalmente por nombre de usuario y por IP. Mediante un backoff exponencial configurable, los administradores del sistema pueden definir el umbral de la lista negra. El objetivo principal de las listas negras es proteger contra los ataques de fuerza bruta a las contraseñas.

Filtrado de direcciones IP (sólo acceso de dispositivos)

Para las conexiones directas (depende de su suscripción), el Servidor RealVNC puede configurarse para impedir las conexiones desde ordenadores con determinadas direcciones IP.

Comprobación manual de identidad (sólo acceso a dispositivos)

Dado que todas las conexiones de datos están cifradas de extremo a extremo, no es posible que un actor dentro de RealVNC monte un ataque pasivo a los datos retransmitidos. Sin embargo, cualquier arquitectura de servicios en la nube que realice la negociación de claves

en nombre de sus clientes puede ser capaz de montar un ataque activo mediante el intercambio de claves falsas. Este ataque permitiría suplantar la identidad de un ordenador del Servidor RealVNC. Véase también la sección Comprobación de identidad, más arriba.

Para protegerse contra un ataque desde dentro de RealVNC al realizar una conexión a la nube, la identidad utilizada para proteger el cifrado de extremo a extremo se presenta opcionalmente al usuario. Esto se muestra como una frase en el Visualizador RealVNC que el usuario debe aprobar. Además, los clientes pueden registrar las identidades, lo que permite a un administrador verificar que no se está realizando ningún ataque activo.

En RealVNC, somos transparentes en cuanto a nuestra seguridad en la nube, y un actor dentro de RealVNC no puede montar un ataque contra un cliente sin dejar un rastro auditable o alertar al usuario a través del cuadro de diálogo de verificación de identidad del Visualizador RealVNC.

Control de acceso (sólo acceso de dispositivos)

Si es probable que un usuario local (es decir, el propietario del Servidor RealVNC) esté físicamente presente mientras se realizan sesiones de control remoto, el Servidor RealVNC puede configurarse para consultar a los usuarios del Visualizador RealVNC a medida que se conectan y solicitar al usuario local que apruebe o rechace cada conexión.

Autenticación multifactor para el Servidor RealVNC (sólo acceso a dispositivos)

El Servidor RealVNC cuenta con varios esquemas de autenticación estándar, que ofrecen uno o dos factores de autenticación. Para las suscripciones de pago, el Servidor RealVNC utiliza la autenticación del sistema de forma predeterminada, por lo que los usuarios del Visualizador RealVNC que se conecten deben introducir el mismo nombre de usuario y contraseña del Directorio Activo o del sistema que utilizan normalmente para iniciar sesión en su escritorio en el equipo remoto. Este esquema puede cambiarse para utilizar:

- Certificados digitales X.509 almacenados en tarjetas inteligentes/tokens de autenticación conectables, o en almacenes de certificados en dispositivos de conexión, de modo que los usuarios del Visualizador RealVNC que se conectan se autentican de forma transparente mediante algo que poseen (una tarjeta inteligente) y algo que conocen (un PIN de tarjeta inteligente).

- La integración nativa de Duo requiere una autenticación adicional a través de Duo por sesión remota.

- Autenticación del sistema aumentada con autenticación RADIUS, por lo que los usuarios del Visualizador RealVNC que se conecten deben introducir primero sus credenciales del sistema y, a continuación, proporcionar un código TOTP u otra credencial, o realizar una o varias operaciones de autorización exigidas por un servidor RADIUS (alojado por un proveedor de gestión de identidades como RSA SecurID).

- Inicio de sesión único (Kerberos- sólo suscripciones Enterprise), para que los usuarios que se conecten al Visualizador RealVNC se autentiquen de forma transparente mediante servicios de red seguros cuando se implementen en la misma LAN y dominio.

- Opcionalmente puede configurarse el inicio de sesión único de Entra ID, y pueden utilizarse políticas de Acceso Condicional para añadir controles adicionales.

- Autenticación interactiva del sistema en Linux y macOS, por lo que los usuarios que se conectan al Visualizador RealVNC deben introducir un nombre de usuario de AD o del sistema y, a continuación, proporcionar credenciales, o realizar operaciones de autorización, exigidas por los módulos PAM.

Además, puede combinar los esquemas de autenticación estándar para crear un esquema personalizado compuesto por tantos factores como necesite.

Permisos de sesión (sólo acceso a dispositivos)

Una vez autenticados correctamente en el Servidor RealVNC, a los usuarios conectados del Visualizador RealVNC se les pueden asignar permisos de sesión por usuario o por grupo, para restringir el acceso a las funciones de control remoto mientras las sesiones están en curso.
Por ejemplo, se puede impedir que determinados usuarios o grupos impriman, transfieran archivos o copien y peguen texto. También se pueden restringir sesiones enteras a solo visualización.

Tiempo de espera

Por defecto, el Servidor RealVNC finaliza las conexiones que no responden después de 1 hora. Este tiempo de espera puede reducirse si es necesario.

Acceso exclusivo (sólo para dispositivos)

Por defecto, el Servidor RealVNC permite la conexión simultánea de cualquier número de usuarios del Visualizador RealVNC. Esto se puede configurar para permitir que sólo un usuario del Visualizador RealVNC se conecte a la vez.

Pantalla en Blanco (sólo acceso al dispositivo)

El Servidor RealVNC puede configurarse para poner en blanco la pantalla de los PC remotos con Windows (que ejecuten Windows 7 o posterior) mientras se realizan sesiones de control remoto, para proteger la privacidad de las operaciones que se realizan a distancia. Estamos trabajando para añadir esta función a otros sistemas operativos y versiones.

Configuración de políticas

Microsoft Group Policy puede utilizarse para bloquear tanto el Visualizador RealVNC como, para el acceso a dispositivos, del Servidor RealVNC. Esto impide la modificación de cualquier opción que haya sido establecida por la política corporativa. En los sistemas UNIX y macOS, se utilizan archivos de configuración de políticas para realizar la misma función. Esto garantiza que los empleados utilicen RealVNC Connect de acuerdo con las políticas corporativas aprobadas. Esta función sólo está disponible en determinados planes de suscripción.

Almacenamiento seguro de credenciales (sólo acceso a dispositivos)

En el Visualizador RealVNC hay una opción para recordar las contraseñas del Servidor RealVNC. Estas se almacenan localmente y nunca se envían a la nube. Si el Visualizador RealVNC está instalado en un equipo Windows, estas contraseñas se almacenan por defecto en la Bóveda de credenciales de Windows. En macOS, se almacenan en el Llavero. En UNIX, están protegidas mediante permisos del sistema de archivos.

En todas las plataformas, es posible establecer una contraseña maestra del Visualizador RealVNC que se utiliza para cifrar las contraseñas individuales del Servidor RealVNC. La clave de cifrado se deriva de la contraseña maestra utilizando PBKDF2 y las entradas se cifran individualmente utilizando AES-GCM-128. Esta capacidad protege el secreto de todas las contraseñas recordadas.

Fijación de certificados raíz

Al establecer una conexión a través de los servicios en la nube de RealVNC, los clientes comprueban el certificado raíz TLS (CA) en una lista blanca. Esto limita la exposición a certificados emitidos por otras autoridades de certificación en el almacenamiento de confianza del SO.

Binarios firmados

En Windows, los instaladores de RealVNC Connect y los binarios instalados se firman mediante Authenticode, mientras que en MacOS utilizamos Gatekeeper. También utilizamos la firma de código para garantizar que el binario no ha sido modificado en tránsito o en reposo por terceros malintencionados. Esto ayuda a evitar la instalación de binarios no autorizados.

Control de la integridad del cliente

Las sumas de comprobación SHA256 se ponen a disposición de los clientes para garantizar la integridad de las descargas de clientes de RealVNC. Las modificaciones de las descargas de clientes son supervisadas por nuestro SOC 24x7 para garantizar que no se realicen cambios no autorizados.

Seguridad en las tiendas de iOS y Android

Nuestras aplicaciones del Visualizador RealVNC y del Servidor RealVNC para iOS y Android han sido probadas por Apple y Google, y firmadas para garantizar su autenticidad. Esto evita la instalación de aplicaciones no autorizadas o fraudulentas.

En RealVNC, somos transparentes en cuanto a nuestra seguridad en la nube, y un actor dentro de RealVNC no puede montar un ataque contra un cliente sin dejar un rastro auditable o alertar al usuario a través del cuadro de diálogo de verificación de identidad del Visualizador RealVNC.

PROCEDIMIENTOS DE DESARROLLO

Visión general

Nuestro equipo de seguridad se ha involucrado constantemente en el desarrollo de RealVNC Connect y sigue participando activamente en el proceso de toma de decisiones tras su lanzamiento.

Nuestro proceso de ciclo de vida de desarrollo de software (SDLC) es un componente de nuestro sistema de gestión de la seguridad de la información (SGSI) y se supervisa y gestiona como parte de nuestra certificación ISO27001.

Antes del desarrollo

Inicialmente establecimos una serie de requisitos de seguridad y privacidad a los que RealVNC Connect debía adherirse. Nuestros principios de seguridad fundamentales -que no tiene que confiar en nosotros para confiar en nuestro software, que el Servidor RealVNC está a cargo de cualquier conexión, que no podemos descifrar sus datos de sesión ni ahora ni en el futuro, y que cualquier conexión activa debe considerarse hostil en todo momento- se establecieron durante estas primeras conversaciones.

A continuación, se llevaron a cabo exhaustivas evaluaciones de los riesgos para la seguridad y la privacidad. Nuevas funciones como la conectividad en la nube y la gestión de cuentas en línea se consideraron de especial riesgo, por lo que se utilizaron modelos de amenazas durante la fase de diseño.

Todo el hardware utilizado para la conectividad en la nube es propiedad y está gestionado exclusivamente por RealVNC, y se almacena en centros de datos remotos que cumplen los estrictos requisitos actuales de certificación y auditoría del sector. Sólo el personal designado de RealVNC tiene capacidad para configurar este hardware. Esto ayuda a mantener al mínimo la superficie de ataque de RealVNC Connect.

Desarrollo

Nuestro equipo de seguridad analiza constantemente nuestro código y sigue revisando el nuevo a medida que se añaden nuevas funciones. Se utilizan herramientas de escaneado de código, así como análisis estáticos manuales, para garantizar que este código se mantiene dentro de los más altos estándares de seguridad posibles. Las revisiones del código garantizan que los desarrolladores no utilicen funciones o prácticas de codificación que se consideren inseguras.
El proceso de revisión del código incluye pruebas fuzz automatizadas de caja blanca, análisis dinámicos con herramientas como Valgrind y AddressSanitizer y una revisión continua de la superficie de ataque de VNC Connect.

El análisis de composición de software (SCA) se utiliza para gestionar las bibliotecas dependientes y garantizar que no existan vulnerabilidades de terceros en los productos RealVNC

Publicación/postdesarrollo

Nuestro código se somete a una última revisión de seguridad antes de cada nueva versión. A continuación, archivamos todos los datos pertinentes. Esto es esencial para que podamos realizar tareas de mantenimiento posteriores a la publicación.

Todos los aspectos de VNC Connect se han diseñado teniendo en cuenta el máximo nivel de seguridad. A pesar de ello, es increíblemente importante que cualquier proveedor de software cuente con un plan de respuesta ante incidentes. Como somos conscientes de que ninguna medida de seguridad es imbatible, podemos lanzar y lanzaremos actualizaciones que protejan nuestro producto de las amenazas que surjan tras su lanzamiento.

Durante más de una década, hemos utilizado CVE para archivar cualquier vulnerabilidad de seguridad de cara al público que hayamos corregido. Seguiremos haciéndolo para VNC Connect, con el fin de seguir siendo lo más transparentes posible para nuestros clientes.

NORMAS Y CUMPLIMIENTOS

La solución de acceso remoto de RealVNC está diseñada para cumplir y ayudar con una amplia gama de normas y regulaciones industriales y gubernamentales. Contamos con la certificación ISO/IEC 27001:2013 y Cyber Essentials y cumplimos con GDPR, y CCPA, garantizando la adhesión a las estrictas directrices de protección de datos y privacidad. Además, RealVNC apoya su cumplimiento con HIPAA y PCI-DSS.

SOC 24x7

Centro de Operaciones de Seguridad (SOC)

Nuestro SOC 24x7 supervisa los eventos de ciberseguridad en toda nuestra infraestructura, investigando y mitigando según sea necesario. La inteligencia global sobre amenazas proporciona información detallada sobre las herramientas, técnicas y tendencias de los atacantes para facilitar un clasificación eficaz.

Certificación ISO/IEC 27001

RealVNC cuenta con la certificación ISO/IEC 27001:2013. ISO 27001 es una norma reconocida internacionalmente para establecer y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta certificación significa que RealVNC ha implantado sistemas para gestionar los riesgos relacionados con la seguridad de los datos que posee o procesa la empresa, y que este sistema cumple los estrictos requisitos de la norma ISO27001.

CYBER ESSENTIALS

Certificación Cyber Essentials

Cyber Essentials es un programa del Centro Nacional de Ciberseguridad del Reino Unido respaldado por el gobierno. La certificación se concede a las empresas británicas que pueden demostrar que disponen de defensas para protegerse contra la gran mayoría de los ciberataques habituales. Para más información, visite **https://www.ncsc.gov.uk/cyberessentials/**

GDPR COMPLIANT

Cumplimiento del GDPR

RealVNC cumple el Reglamento General de Protección de Datos (RGPD)

CCPA COMPLIANT

Cumplimiento de la CCPA

RealVNC cumple con la Ley de Privacidad del Consumidor de California (CCPA).

PCI DSS COMPLIANCE

HIPAA COMPLIANCE

Apoyo para el cumplimiento de las normas HIPAA y PCI-DSS

Para obtener información detallada sobre cómo RealVNC puede ayudarle a cumplir las normativas HIPAA y PCI-DSS, consulte la documentación específica disponible en **https://www.realvnc.com/es/connect/security/**

RESUMEN

Las funciones y procesos de seguridad que protegen RealVNC Connect forman parte de una estrategia en profundidad. En este documento se ha intentado explicar esta estrategia separándola en cuatro categorías clave.
Confiamos en que esto haya contribuido a arrojar algo de luz sobre nuestra seguridad y a ilustrar la integridad de nuestro enfoque. Sin embargo, dada la complejidad inherente a la seguridad de los programas informáticos, entendemos que pueda tener preguntas específicas. No dude en ponerse en contacto con nosotros. Estaremos encantados de ponerle en contacto con el miembro adecuado de nuestro equipo de desarrollo.

Si tiene alguna pregunta sobre los temas planteados en este documento técnico, póngase en contacto con nosotros en **enquiries@realvnc.com** o visite **realvnc.com/contact-us.**

www.realvnc.com

El software de acceso remoto y gestión de RealVNC es utilizado por cientos de millones de personas en todo el mundo en todos los sectores de la industria, la administración pública y la educación. Nuestro software ayuda a las organizaciones a reducir costes y mejorar la calidad del soporte de ordenadores y aplicaciones remotas. RealVNC es el desarrollador original del software de acceso remoto VNC y es compatible con una combinación inigualable de plataformas de escritorio y móviles. Mediante el uso de nuestros SDK de software, las empresas tecnológicas de terceros también integran la tecnología de acceso remoto directamente en sus productos a través de acuerdos OEM.

www.realvnc.com