Nro. Alerta:	EC-2022-084	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	17-ago-2022	Servidores VNC expuestos a internet, permiten fácil acceso no autorizado	V 1.0

I. DATOS GENERALES:

Clase de alerta: Otros

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Bajo

II. ALERTA:

Los investigadores han descubierto al menos 9000 puntos finales VNC (Virtual Network Computing) expuestos, a los que se puede acceder y utilizar sin autenticación, lo que permite a los actores de amenazas, acceder fácilmente a estaciones de trabajo y redes internas.

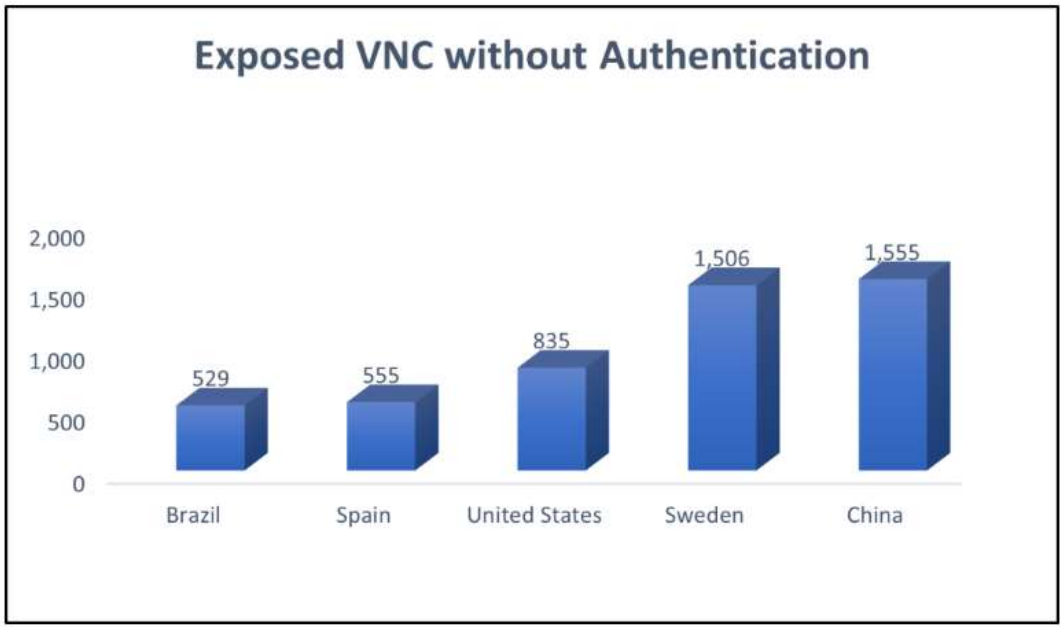

Figura 1: Los principales países con VNC expuestos. Fuente: Cyble Inc.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-084	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	17-ago-2022	Servidores VNC expuestos a internet, permiten fácil acceso no autorizado	V 1.0

III. INTRODUCCIÓN:

Virtual Network Computing (VNC) es un software de acceso remoto que utiliza el protocolo Remote Frame Buffer (RFB); compatible con cualquier sistema operativo.

Un sistema VNC consta de un servidor instalado en el dispositivo que se conecta de forma remota por red y un cliente de control; de forma predeterminada, los servicios VNC utilizan el puerto TCP 5900.

Dependiendo de qué sistemas se encuentran detrás de los VNC expuestos, las consecuencias podrían ser devastadoras para las empresas ya que se puede acceder a todos los archivos e información disponible en las computadoras de una red.

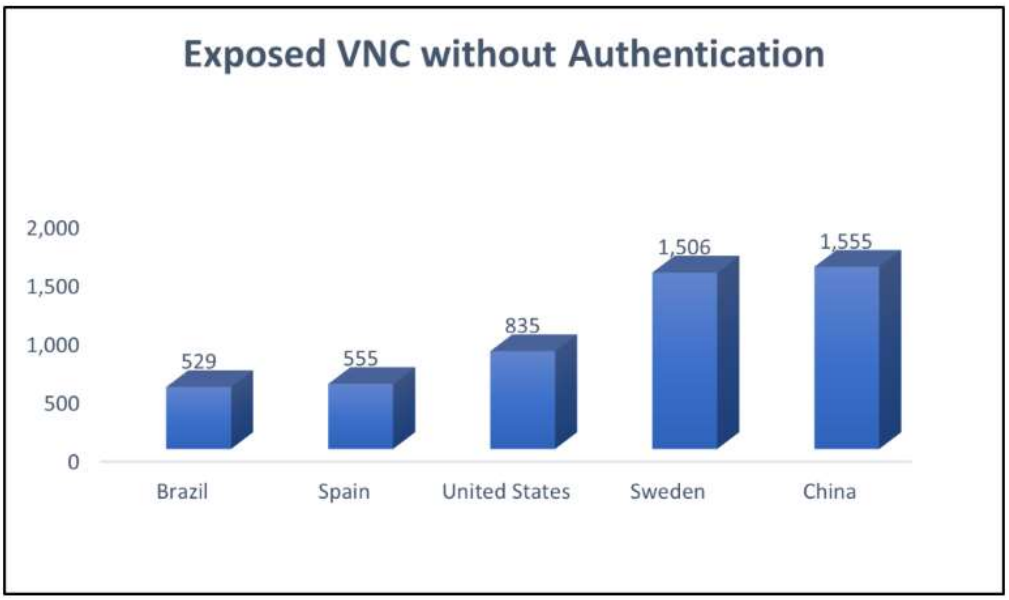

Figura 2: los 5 principales países con VNC expuestos

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-084	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	17-ago-2022	Servidores VNC expuestos a internet, permiten fácil acceso no autorizado	V 1.0

El hacker con el apodo de Spielerkid89 usó el motor de búsqueda Shodan para buscar computadoras a las que se pudiera acceder a través de Internet; descubriendo un puerto VNC abierto con autenticación deshabilitada. El computador expuesto, pertenecía al ministerio de salud en la región de Omsk en Rusia según lo confirmó el equipo de investigación de Cybernews, que fue contactado por el hacker.

Aunque VNC ofrece muchas configuraciones de seguridad, a veces los administradores del sistema las pasan por alto y dejan puertos abiertos con la autenticación deshabilitada. Además, productos VNC no admiten contraseñas de más de ocho caracteres, por lo que son intrínsecamente inseguros incluso cuando las sesiones y las contraseñas están habilitadas y encriptadas.

IV. VECTOR DE ATAQUE: Red

V. IMPACTO:

La demanda de acceso a redes críticas a través de VNC expuestas es alta en los foros de hackers, debido a que este tipo de acceso puede en determinadas circunstancias utilizarse para una infiltración más profunda de la red. Personas mal intencionadas pueden utilizar el VNC para realizar acciones maliciosas con el usuario que inició sesión tales como: acceso no autorizado a documentos, ejecutar comandos arbitrarios, robo de información, configuración de puertas traseras, instalación de troyanos de acceso remoto, movimientos laterales a otros dispositivos en la red o la limpieza de los dispositivos objetivo, etc.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-084	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	17-ago-2022	Servidores VNC expuestos a internet, permiten fácil acceso no autorizado	V 1.0

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Uso de VPNs para asegurar que solo personal autorizado tenga acceso a los servidores.
- Utilizar la autenticación multifactor (MFA) para servidores VNC.
- Revisar los registros de conexión periódicamente.
- Establezca una contraseña única y compleja para su servidor VNC y reemplácela con frecuencia.

VII. DESCARGO DE RESPONSABILIDAD:

- La información en la presente alerta; se proporciona solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-084	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	17-ago-2022	Servidores VNC expuestos a internet, permiten fácil acceso no autorizado	V 1.0

VIII. REFERENCIAS BIBLIOGRÁFICAS:

Constantinescu, V. (2022 de mar de 2022). *Bitdefender*. Obtenido de https://www-bitdefender-com.translate.goog/blog/hotforsecurity/hacker-breaches-russian-ministry-computer-through-unsecured-vnc-ports/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=op,sc

Cyble Inc. (12 de ago de 2022). *Cyble Inc*. Obtenido de https://blog.cyble.com/2022/08/12/exposed-vnc-a-major-threat-to-critical-infrastructure-sectors/

Hackwise. (16 de ago de 2022). *Hackwise*. Obtenido de https://hackwise.mx/mas-de-9000-servidores-vnc-estan-expuestos-en-linea-sin-contrasena/

Lapienytė, J. (21 de mar de 2022). *Cybernews*. Obtenido de https://cybernews.com/cyber-war/hacker-breaches-key-russian-ministry-in-blink-of-an-eye/

Toulas, B. (14 de ago de 2022). *Bleeping Computer*. Obtenido de https://www.bleepingcomputer.com/news/security/over-9-000-vnc-servers-exposed-online-without-a-password/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec