Accessible RDP Services (Remote Desktop Protocol,RDP)

1. PROTOCOLO DE ESCRITORIO REMOTO (RDP)

Es un protocolo propietario desarrollado por Microsoft que proporciona capacidades de visualización y de entrada remotos a través de conexiones de red para aplicaciones basadas en Windows que se ejecutan en un servidor. RDP está diseñado para soportar diferentes tipos de topologías de red y múltiples protocolos de LAN. Permite la comunicación en la ejecución de una aplicación entre un terminal (muestra la información procesada que recibe del servidor) y un servidor Windows (recibe la información dada por el usuario en el terminal mediante el mouse o el teclado).

La información gráfica que genera el servidor es convertida a un formato RDP y enviada a través de la red al terminal, que interpreta la información contenida en el paquete del protocolo para reconstruir la imagen en la pantalla del terminal. En le envío de comandos a través del terminal, las teclas que pulsa el usuario en el teclado del terminal, movimientos y pulsaciones del mouse son redirigidos al servidor. El protocolo también permite que toda la información que intercambien cliente y servidor sea comprimida para un mejor rendimiento así como también es cifrada para seguridad.

Este servicio utiliza por defecto el puerto TCP 3389 en el servidor para recibir las peticiones. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de windows, no se observará que el usuario está trabajando forma remota.

2. RIESGO

El RDP mal configurado puede permitir a intrusos acceder al escritorio de un host vulnerable y también permitir la recopilación de información en un host de destino, ya que el certificado SSL utilizado por RDP a menudo contiene el nombre de host del sistema.

Exponer RDP a conexiones directas es arriesgado, ya que no sólo ofrece a los atacantes remotos la oportunidad de adivinar las credenciales de inicio de sesión, sino que también depende de vulnerabilidades remotamente explotables en la implementación de RDP de Microsoft.

El boletín de seguridad MS12-020 de Microsoft , publicado en marzo de 2012, describió una vulnerabilidad crítica en la implementación RDP de Microsoft en la mayoría de las plataformas Windows (CVE-2012-0002). Este error permitía a un atacante no autenticado remoto ejecutar código arbitrario en el sistema afectado enviando "una secuencia de paquetes RDP especialmente diseñados".

3. DETECCIÓN

Este informe identifica a los hosts que tienen el servicio de escritorio remoto (RDP) en ejecución y está accesible en Internet. El comando shell para verificar si el puerto 3389 está abierto es:

nmap -v --script=ssl-cert -p 3389 [IP]

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Nombre de la vulnerabilidad reportada
Dirección IP	Dirección IP del host
Puerto	Puerto desde donde se obtiene la respuesta
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
status_EcuCERT	Online: vulnerabilidad reportada por *Feeds* y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por *Feeds*, pero en el timestamp_EcuCERT no se detectó.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del dispositivo en cuestión
protocol	Protocolo por el que ingresó la respuesta (siempre TCP)
port	Puerto desde donde se obtiene la respuesta (3389/TCP)
hostname	DNS reverso del host
tag	Siempre será telnet
asn	ASN de la red donde se encuentra el host
geo	País donde se encuentra el host
region	Estado/Provincia/Región donde se encuentra el host
city	Ciudad donde se encuentra el host
rdp_protocol	Versión del protocolo RDP que responde.
cert_length	Longitud del certificado (1024, 2048, 4096, etc)
subject_common_name	El nombre del certificado SSL
issuer_common_name	Nombre de la entidad que firmó el certificado SSL
cert_issue_date	Fecha cuando el certificado SSL fue válido
cert_expiration_date	Fecha cuando el certificado SSL expira
sha1_fingerprint	Huella SHA1 del certificado
cert_serial_number	Número de serie embebido del certificado
ssl_version	Versión SSL

Campo	Descripción
signature_algorithm	Algoritmo utilizado para firmar el certificado
key_algorithm	Algoritmo utilizado por la llave
sha256_fingerprint	Huella SHA256 del certificado
sha512_fingerprint	Huella SHA512 del certificado
md5_fingerprint	Huella MD5 del certificado
naics	Código del Sistema de Clasificación Industrial de América del Norte
sic	Código del Sistema de Clasificación Industrial Estándar

4. ACCIONES RECOMENDADAS

Para evitar este tipo de vulnerabilidad se recomienda:

- Si no se utiliza el servicio RDP, es recomendable desactivarlo un sistema que no tenga habilitado este servicio, no es vulnerable. Mayor información en https://technet.microsoft.com/es-es/library/cc731588(v=ws.11).aspx
- Mantener actualizado el sistema operativo de manera periódica.
- Configurar una regla utilizando el firewall de Windows para evitar accesos indebidos al servicio.
- En caso de tener duda si se cuenta con la actualización correspondiente, puede dirigirse al sitio de RDPCheck y comprobar si su sistema es vulnerable o no ingresando su IP.
- Cambie el puerto en el que sus sistemas escuchan la conexión RDP para evitar el uso del puerto TCP 3389 predeterminado. Los escáneres y los gusanos automatizados tendrán menos posibilidades de ubicar RDP en puertos de alto nivel no estándar.
- Usar autenticación robusta para los sistemas que utilizan RDP para hacer frente a los ataques de detección remota de contraseñas.

5. REFERENCIAS

- https://www.shadowserver.org/wiki/pmwiki.php/Services/Accessible-RDP/
- https://es.wikipedia.org/wiki/Remote_Desktop_Protocol
- http://www.welivesecurity.com/la-es/2012/03/20/grave-vulnerabilidad-ms12-020-sistemas-microsoft/
- https://ocubom.wordpress.com/2012/04/04/proteger-la-conexion-al-escritorio-remoto-en-windows/
- https://social.technet.microsoft.com/Forums/es-ES/81c3e9d6-1547-4f01-a82f-7280df2477b7/posibles-vulnerabilidades-en-terminal-server?forum=wstses