GUÍA TÉCNICA PRACTICAS INSTRUCTOR

MÓDULO 17. TALLER 1

TALLER 1: ELABORACIÓN REPORTE

Elaboración de un reporte técnico y ejecutivo de un proceso de evaluación de seguridad. Usted es un pentester y acaba de encontrar la siguiente vulnerabilidad:

VULNERABILIDAD OpenSSH.

Según el informe del INCIBE con fecha 19/12/2023, las versiones de OpenSSH anteriores a la 9.6, sufren múltiples vulnerabilidades de importancia 4 (Alta).

Descripción

Se ha publicado la versión 9.6 de OpenSSH, que contiene una serie de correcciones de seguridad, destacando 3 vulnerabilidades descubiertas por los investigadores Fabian Bäumer, Marcus Brinkmann y Jörg Schwenk, de la Universidad Ruhr de Bochum, y que se ha denominado Terrapin Attack. La explotación de estas vulnerabilidades podría permitir un ataque MitM que rompiese la integridad del canal seguro de SSH.

Listado de referencias

OpenSSH 9.6

Terrapin Attack

Terrapin Vulnerability Scanner

Realizar el informe donde describa a la alta gerencia que sucedió y qué tan peligroso es esta vulnerabilidad.

Reporte sobre vulnerabilidad OpenSSH (19/12/2023)

JOAQUIM CHAGAS NETO

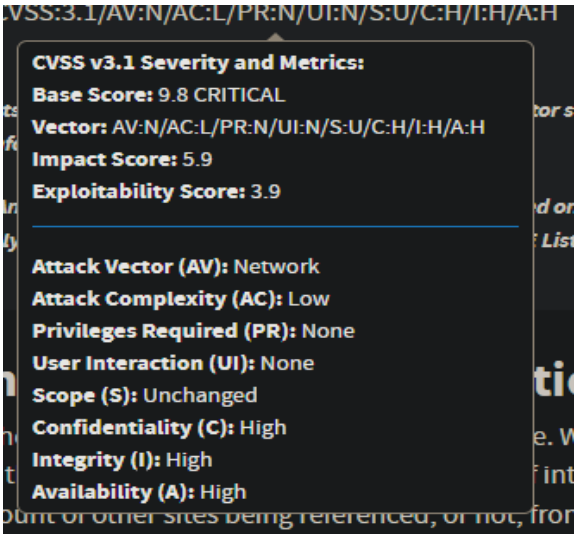
Sumario.

Investigación sobre una vulnerabilidad detectada en OpenSSH que da lugar a posibles ataques de Man In The Middle (MITM). Permite a los atacantes acceder remotamente al sistema y ejecutar comandos con la finalidad de obtener información.

Información técnica.

Esta vulnerabilidad está siendo investigada con el identificador CVE-2023-38408, afectando a las versiones anteriores a la 9.3 de OpenSSH.

Se trata de una vulnerabilidad crítica con un base score del 9.8. Con un vector de ataque mediante la red, una complejidad de ejecución baja, no se requieren privilegios de ejecución tampoco de interacciones con el usuario.



Su impacto en la confidencialidad, disponibilidad e integridad es alto.

Mediante un ataque llamado “Terrapin”, un atacante puede rebajar la seguridad de la conexión truncando el mensaje de negociación de extensión de la transcripción. Esto da lugar a la utilización de algoritmos de autenticación menos seguros

y desactivar contramedidas específicas contra ataques de sincronización de pulsaciones de teclas en OpenSSH.

Además, mediante el ataque de Terrapin se encontraron fallos en los servidores AsyncSSH permitiendo a un atacante iniciar sesión en el cliente de la víctima en otra máquina sin que se de cuenta. Supone un gran problema, ya que, permite ataques de phishing y de MITM dentro de esta sesión.

Para realizar el ataque Terrapin, el atacante debe interceptar y modificar el tráfico de la conexión; que la conexión esté protegida por ChaCha20-Poly1305 o CBC con Encrypt-then-MAC.

Mientras que se ha probado la Prueba de Concepto (PoC), no hay evidencias de que este ataque ha sido llevado a cabo en el mundo real.

Métodos de prevención.

Mediante un Scanner basado en Go, se puede averiguar si un servidor o cliente de SSH es vulnerable a este ataque.

Si somos vulnerables, deberemos de seguir las siguientes indicaciones para tratar de minimizar las posibilidades de sufrir un ataque de este tipo. Las indicaciones a seguir son:

1. Actualizar OpenSSH a una versión posterior a la 9.3+.
2. Restringir proveedores de PKCS#11 (Public-Key Cryptography Standards).
3. Tener cuidado en el reenvío de agentes de SSH a servidores o entornos que no sean de confianza.
4. Realizar análisis del sistema regularmente usando antivirus y detectores de malware como CLAMAV, Malwarebytes…
5. Gestionar claves para la autenticación sin contraseña.
6. Deshabilitar utilización de contraseñas vacías.
7. Limitar el número de intentos fallidos en una sesión.
8. Crear una whitelist de usuarios autorizados.
9. Cambiar el puerto del protocolo SSH por defecto.
10. Limitar el número de conexiones simultáneas de un usuario.

Conclusión.

La vulnerabilidad descubierta de OpenSSH supone un gran riesgo para los datos sensibles de cualquier usuario ya que tiene un impacto crítico en la confidencialidad, disponibilidad e integridad de estos.

SSH es un protocolo bastante extendido en el mundo por su seguridad y esto hace que cualquiera este expuesto a ser atacado.

Para mitigar su posible explotación es recomendable que seguir las medidas de prevención anteriormente expuestas y tratar de usar el sentido común.

REPORTE EJECUTIVO DE VULNERABILIDAD EN OPENSSH

Sumario.

Identificación de una vulnerabilidad crítica en el software OpenSSH, una implementación ampliamente utilizada del protocolo SSH (Secure Shell). La vulnerabilidad detectada presenta riesgos significativos de ataques Man-in-the-Middle (MITM) y de phishing, comprometiendo la integridad y confidencialidad de las comunicaciones seguras a través de SSH.

Descripción.

Vulnerabilidad en la validación adecuada de la autenticidad del servidor SSH durante la negociación de la clave pública. Esto permite que un atacante lleve a cabo ataques Man in the Middle, interceptando y manipulando las comunicaciones entre el cliente y el servidor SSH sin ser detectado. Además, la falta de autenticación adecuada podría facilitar ataques de phishing.

Consecuencias.

Si el atacante consigue realizar un ataque exitoso puede realizar:

- Interceptaciones sobre las comunicaciones confidenciales entre servidor y cliente SSH.
- Ataques phishing para conseguir credenciales.
- Poner en riesgo la confidencialidad, disponibilidad e integridad de los datos transmitidos mediante SSH.

Prevención.

Es recomendable seguir los siguientes pasos para minimizar el posible ataque lo máximo posible. Entre ellos:

- Actualizar OpenSSH de una fuente segura a la última versión ya que en esta se corrigen los fallos de seguridad.
- Monitorear el tráfico SSH para evitar ataques o escuchas indebidas provocadas por un ataque Man in the Middle.
- Proporcionar una hoja de ruta a los usuarios involucrados en el área de seguridad para tener una buena higiene a la hora de utilizar este tipo de conexión evitando filtraciones de credenciales.
- Si no fuese posible lo anterior, evitar utilizar el protocolo SSH hasta nuevo aviso; esperar nuevos parches de seguridad, utilizar otros medios, etc…

Conclusión.

Es de vital importancia mantener actualizado el protocolo OpenSSH ya que si un atacante logra entrar en el sistema mediante el protocolo SSH puede retener información valiosa de cualquier sistema afectado, llegando a poner en serios problemas la integridad, confidencialidad y disponibilidad de sus datos.

Aplicar las recomendaciones para la prevención del riesgo hallado reducirá el riesgo de exposición a ataques MITM y de phishing, pero no se eliminará el riesgo al 100%.

Este informe se ha elaborado con la finalidad de informar y sobre todo para mitigar los riesgos provocados por la vulnerabilidad.