BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-01
Fecha de publicación: 00/01/2024
Tema: Ataque Terrapin que afecta al protocolo SSH
Traffic Light Protocol (TLP): White

Producto afectado:

- OpenSSH versión 9.5 y menores

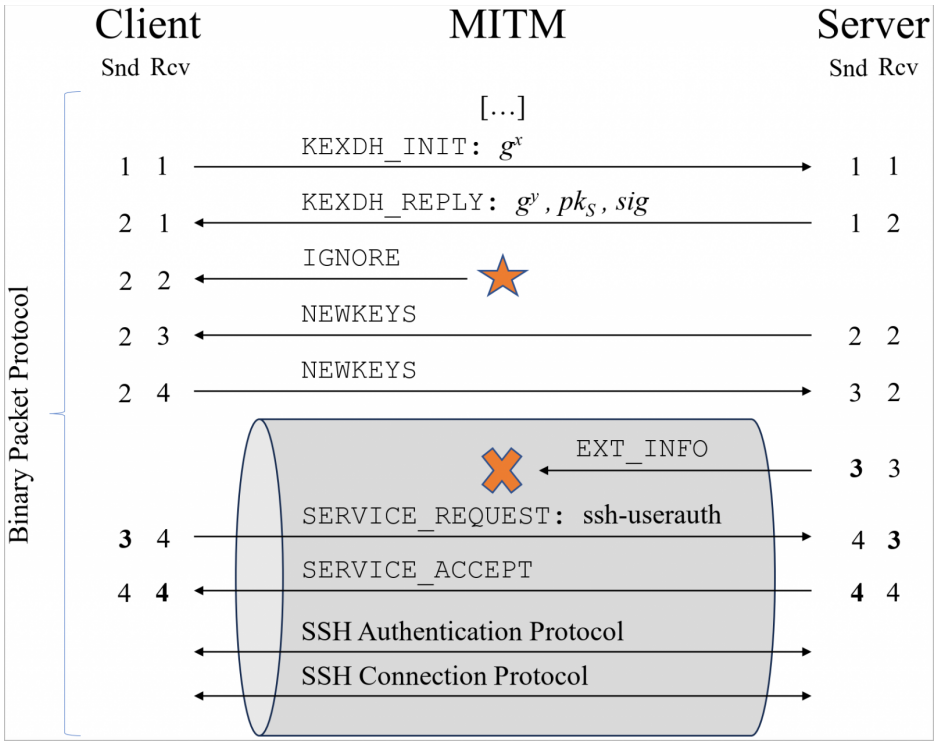
Descripción:

Se ha reportado un nuevo ataque que afecta al estándar de conexión remota SSH, el mismo fue desarrollado por investigadores académicos de la Universidad Ruhr de Bochum los cuales desarrollaron un nuevo ataque llamado Terrapin que manipula números de secuencia durante el proceso de intercambio (handshake) para romper la integridad del canal SSH cuando se utilizan ciertos modos de cifrado ampliamente utilizados. Las debilidades y fallas asociadas con el ataque se identifican como CVE-2023-48795, CVE-2023-46445 y CVE-2023-46446.

Esta manipulación permite a los atacantes eliminar o modificar mensajes intercambiados a través del canal de comunicación, lo que lleva a degradar los algoritmos de clave pública utilizados para la autenticación de usuarios o deshabilitar las defensas contra ataques de sincronización de pulsaciones de teclas en OpenSSH 9.5. Un ataque Terrapin reduce la seguridad de la conexión establecida al cortar mensajes de negociación importantes sin que el cliente o el servidor se dé cuenta.

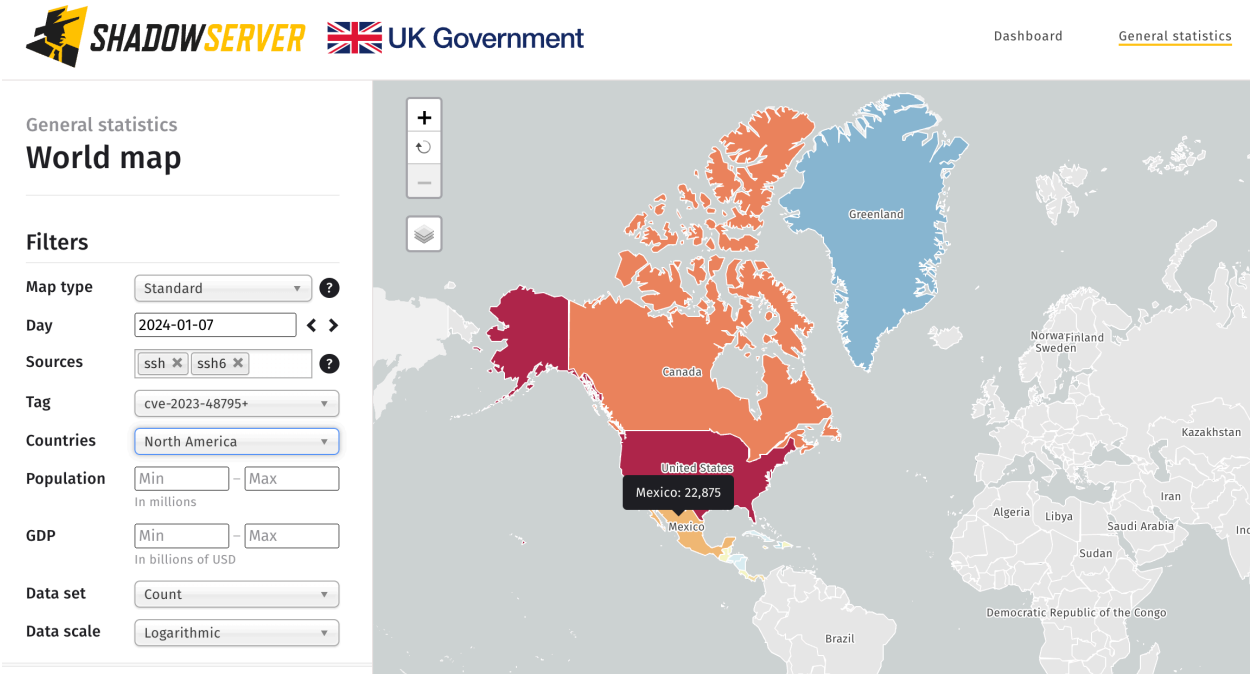
Una cosa a tener en cuenta sobre Terrapin es que los atacantes deben estar en una posición de Man-in-The-Middle (MiTM) en la capa de red para interceptar y modificar el intercambio de protocolo de enlace, y la conexión debe estar asegurada por ChaCha20-Poly1305 o CBC con Encrypt-luego-MAC.

Los datos de los mensajes intercambiados después de completar el protocolo de enlace determinan la gravedad de las repercusiones del ataque.



"El ataque Terrapin explota las debilidades en el protocolo de la capa de transporte SSH en combinación con algoritmos criptográficos y modos de cifrado más nuevos introducidos por OpenSSH hace más de 10 años", dicen los investigadores , y agregan que "estos han sido adoptados por una amplia gama de implementaciones SSH, por lo tanto afectando a la mayoría de las implementaciones actuales".

Se estima que exiten mas de 11 millones dispositivos vulnerables al ataque Terrapin, 22.875 solo en México.



Impacto

La ejecución del ataque en OpenSSH para demostrar el impacto de la vulnerabilidad puede provocar problemas de autenticación del usuario y combinado con Timing Channel Attack puede podría ser explotado para deducir la longitud exacta de la contraseña de un usuario y luego utilizar pulsaciones precisas entre teclas, momento para descifrar la contraseña

Mitigación

El equipo ha publicado un escáner de vulnerabilidad Terrapin en GitHub , que los administradores pueden utilizar para determinar si un cliente o servidor SSH es vulnerable al ataque.

Dado que el éxito del ataque depende del la intersección de la conexión por MiTM, buenas prácticas para evitar MiTM serán mas que util para prevenir el ataque.

Para evitar ataques de Man-in-the-Middle (MitM) en conexiones SSH, se pueden seguir algunas buenas prácticas:

1. Verificar las claves de host: Al conectarte a un servidor SSH por primera vez, se genera y almacena una clave de host en tu cliente SSH. En futuras conexiones, el servidor SSH enviará su clave de host para verificarla con la clave almacenada en el cliente. Si la clave no coincide, es posible que estés siendo víctima de un ataque MitM. Siempre debes verificar cuidadosamente la clave de host antes de aceptarla.
2. Usar autenticación de clave pública: La autenticación de clave pública es más segura que la autenticación basada en contraseñas. Genera un par de claves (pública y privada) en tu cliente y guarda la clave pública en el servidor SSH al que te conectas. Esto te permite autenticarte sin necesidad de ingresar una contraseña cada vez. Además, la autenticación de clave pública es más resistente a los ataques MitM.
3. Evitar el acceso a servidores SSH públicos: Los servidores SSH públicos son más propensos a ser blanco de ataques MitM. Es preferible evitar conectarse a servidores SSH públicos, especialmente aquellos que no requieren autenticación segura.
4. Utilizar una VPN: Una forma adicional de proteger las conexiones SSH contra ataques MitM es utilizar una VPN (Red Privada Virtual, por sus siglas en inglés). Una VPN cifra todo el tráfico entre tu dispositivo y el servidor SSH, lo que dificulta que un atacante intercepte y manipule los datos.
5. Limitar los puertos de escucha: En el servidor SSH, restringe los puertos de escucha solo a aquellos necesarios. Esto reducirá la superficie de ataque y disminuirá las posibilidades de que un atacante pueda interceptar la conexión SSH.
6. Activar **StrickHostKeyChecking Yes** en tu ~/.ssh/config. Puede ser molestoso para nuevas conexiones.

Para mitigar CVE-2023-48795 sin actualizar deshabilite el ChaCha20-Poly1305cifrado vulnerable en las configuraciones del cliente y del servidor OpenSSH. Específicamente, agregue lo siguiente linea al /etc/ssh/ssh(d)_config:

```
Ciphers -chacha20-poly1305@openssh.com
```

Luego, reinicie su servidor SSH.

Solución

OpenSSH solucionó este problema en la versión 9.6p1 y corresponden directamente a las sugerencias hechas por los investigadores. Como se menciona en las notas de la versión de SSH, cualquiera de estos cambios debería ser suficiente para detener Terrapin Attack. Recomendamos actualizar sus servidores SSH.

Información adicional:

- https://www.bleepingcomputer.com/news/security/terrapin-attacks-can-downgrade-security-of-openssh-connections/
- https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/nearly-11-million-ssh-servers-vulnerable-to-new-terrapin-attacks/amp/
- https://dashboard.shadowserver.org/statistics/combined/map/?map_type=std&day=2024-01-07&source=ssh&source=ssh6&tag=cve-2023-48795%2B&geo=North+America&data_set=count&scale=log
- https://terrapin-attack.com/
- https://jfrog.com/blog/ssh-protocol-flaw-terrapin-attack-cve-2023-48795-all-you-need-to-know/#:~:text=JFrog%20Advanced%20Security-,Affected%20Implementations,%2C%20FileZilla%2C%20and%20many%20more.

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com