BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-18
Fecha de publicación: 01/07/2024
Tema: Vulnerabilidad regreSSHion, CVE-2024-6387
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Versiones anteriores a 4.4p1: Son susceptibles a esta vulnerabilidad si no cuentan con los parches para CVE-2006-5051 y CVE-2008-4109.

- Versiones desde 8.5p1 hasta 9.8p1, sin incluirla: La vulnerabilidad resurge debido a la eliminación accidental de un componente crítico en una función.

Descripción

La Unidad de Investigación de Amenazas de Qualys (TRU) ha descubierto una grave vulnerabilidad denominada "regreSSHion" (CVE-2024-6387) que afecta al servidor OpenSSH (sshd) en sistemas Linux basados en glibc. Esta falla, una condición de carrera en el controlador de señales, permite a atacantes no autenticados obtener acceso root y tomar control total de las máquinas vulnerables. La vulnerabilidad es una regresión de CVE-2006-5051, una falla previamente corregida que ha reaparecido en versiones posteriores.

Los investigadores que han desarrollado un exploit para AMD64 señalan que, debido a que la explotación requiere varias rondas de intentos hasta conseguir ganar la carrera, así como también debido a las protecciones ASLR normalmente presentes, la explotación exitosa es compleja y lenta. En las pruebas realizadas les tomó una semana en obtener un shell de root en la versión x86 (32 bits). No se ha probado para x64 (64 bits).

Diversos investigadores publicaron recursos que podrían ser de utilidad, como por ej el siguiente scanner, que puede ser utilizado para verificar si está afectado por la vulnerabilidad: https://github.com/xaitax/CVE-2024-6387_Check

Impacto

La explotación exitosa de la vulnerabilidad "regreSSHion" podría tener consecuencias devastadoras:

- Compromiso del Sistema Completo: Los atacantes pueden instalar malware, manipular datos y establecer puertas traseras para acceso persistente.

- Propagación en la Red: La vulnerabilidad permite a los atacantes eludir los mecanismos de seguridad y propagarse a través de la red, poniendo en riesgo tanto a empresas como a individuos.

Mitigación

- Actualizar OpenSSH a la versión 9.8p1 que corrige la vulnerabilidad.

Controles compensatorios

- Modificar Configuración de sshd: Si no es posible actualizar o recompilar sshd, configure LoginGraceTime a 0 en el archivo de configuración de sshd. Esto hará que sshd sea vulnerable a una denegación de servicio, pero mitigará la posibilidad de ejecución remota de código.
- Restringir el acceso SSH
    - Configurar firewalls para limitar el acceso SSH solo a las direcciones IP autorizadas.
    - Bloquear el acceso SSH desde ubicaciones no seguras o innecesarias
    - Limitar el acceso SSH a servidores específicos dentro de esos segmentos.
    - Permitir el acceso SSH únicamente desde una lista predefinida de direcciones IP de confianza.

Información adicional:

- https://www.openssh.com/releasenotes.html
- https://www.qualys.com/regresshion-cve-2024-6387/
- https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6387
- https://bugzilla.redhat.com/show_bug.cgi?id=2294604

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com