BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-03
Fecha de publicación: 13/01/2025
Tema: Juniper Networks corrige vulnerabilidades críticas en Junos OS

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Junos OS, en versiones 21.2R3-S8, 21.4R3-S7, 22.2R3-S4, 22.3R3-S2, 22.4R3, 23.2R2, 23.4R1, 24.2R1
- Junos OS Evolved, desde 24.2-EVO antes de 24.2R1-S2-EVO, 24.2R2-EVO
- Junos Space 24.1R2

Descripción

Juniper Networks ha publicado actualizaciones de seguridad para su sistema operativo Junos OS, abordando múltiples vulnerabilidades de alta severidad que podrían ser explotadas para causar condiciones de denegación de servicio (DoS).

Las vulnerabilidades más críticas que se han parcheado que son la CVE-2025-21598 y CVE-2025-21599, son las siguientes:

CVE-2025-21598:
Esta es una vulnerabilidad que afecta a los sistemas que tienen habilitadas las opciones de seguimiento de recepción de paquetes y puede propagarse y multiplicarse a través de múltiples ASes hasta llegar a los dispositivos vulnerables. Como solución alternativa se debe desactivar las opciones de rastreo de paquetes. Para detectar posibles vulnerabilidades, deben buscar mensajes de actualización mal formados en dispositivos AS vecinos que no estén afectados.

CVE-2025-21599:
Un defecto de seguridad crítica en el Juniper Tunnel Driver (JTD) de Junos OS Evolved que permite que paquetes IPv6 específicamente malformados y que podrían explotarse a través de la red, causen agotamiento de memoria en el kernel, llevando a un bloqueo del sistema y DoS.

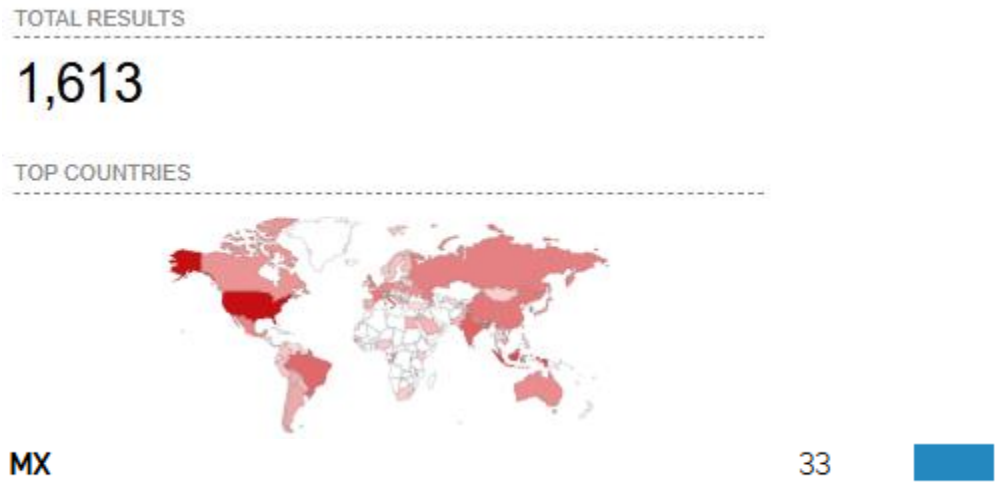
CVE-2024-6387 (regreSSHion) y CVE-2024-39894:

Estas vulnerabilidades de alta severidad en OpenSSH utilizado en Junos OS y Junos OS Evolved, que podrían ser explotadas para comprometer la seguridad del sistema.

Se descubrió una regresión de seguridad (CVE-2006-5051) en el servidor de OpenSSH (sshd). Existe una condición de carrera que puede hacer que sshd maneje algunas señales de manera insegura. Un atacante remoto no autenticado podría ser capaz de activarla si no se autentica dentro de un período de tiempo determinado.

OpenSSH 9.5 a 9.7 antes de 9.8 a veces permite ataques de tiempo contra la entrada de contraseñas sin eco (por ejemplo, para su y Sudo) debido a un error de lógica ObscureKeystrokeTiming. De manera similar, podrían ocurrir otros ataques de tiempo contra la entrada de teclas.

Según datos de Shodan, se han identificado algunas decenas de equipos Juniper expuestos a Internet. El siguiente mapa global muestra que los dispositivos más vulnerables se encuentran en Estados Unidos, UK, Canada y México, encontrando en este último 519 dispositivos.



La semana pasada, Juniper también anunció que se lanzó Junos Space 24.1R2 con parches para casi 60 fallas en componentes de terceros, incluidos problemas de gravedad crítica en Expat (libexpat), una biblioteca de análisis XML orientada a flujos.

Ninguna de estas vulnerabilidades parece ser explotada en la red, pero se recomienda a los usuarios que apliquen los parches disponibles lo antes posible, ya que no es raro que los actores de amenazas se centren en las fallas del sistema operativo Junos.

Solución

Se recomienda encarecidamente a los usuarios y administradores de sistemas actualizar sus dispositivos a las versiones más recientes de Junos OS, Junos OS Evolved y Junos Space, donde estas vulnerabilidades han sido corregidas. Además, como medida temporal, se sugiere desactivar las opciones de rastreo de paquetes para mitigar posibles explotaciones.

Puede encontrar información adicional en la página de avisos de seguridad de Juniper Networks.

Información adicional:

- https://www.securityweek.com/juniper-networks-fixes-high-severity-vulnerabilities-in-junos-os/
- https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-vulnerabilities-resolved-in-OpenSSH?language=en_US
- https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-When-BGP-traceoptions-are-configured-receipt-of-malformed-BGP-packets-causes-RPD-to-crash-CVE-2025-21598?language=en_US

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com