Juniper Networks ha publicado actualizaciones de seguridad para solucionar una grave vulnerabilidad que afecta a los dispositivos Session Smart Router, Session Smart Conductor y WAN Assurance Router, la cual podría ser aprovechada para tomar el control de los equipos vulnerables.

Catalogada como CVE-2025-21589, la vulnerabilidad posee una puntuación CVSS v3.1 de 9.8 y CVSS v4 de 9.3.

> *«Una vulnerabilidad de elusión de autenticación a través de un camino o canal alternativo en el Session Smart Router de Juniper Networks puede permitir que un atacante en la red eluda la autenticación y adquiera control administrativo del dispositivo»*, señaló la empresa en un comunicado.

Los productos y versiones afectados son los siguientes:

- Session Smart Router: Desde la versión 5.6.7 hasta 5.6.16, desde 6.0.8, desde 6.1 hasta 6.1.11-lts, desde 6.2 hasta 6.2.7-lts, y desde 6.3 hasta 6.3.2-r2.
- Session Smart Conductor: Desde la versión 5.6.7 hasta 5.6.16, desde 6.0.8, desde 6.1 hasta 6.1.11-lts, desde 6.2 hasta 6.2.7-lts, y desde 6.3 hasta 6.3.2-r2.
- WAN Assurance Managed Routers: Desde la versión 5.6.7 hasta 5.6.16, desde 6.0.8, desde 6.1 hasta 6.1.11-lts, desde 6.2 hasta 6.2.7-lts, y desde 6.3 hasta 6.3.2-r2.

Juniper Networks mencionó que la vulnerabilidad fue descubierta durante pruebas de seguridad internas de sus productos y aseguró que no tiene conocimiento de que haya sido explotada maliciosamente.

La falla ha sido corregida en las versiones SSR-5.6.17, SSR-6.1.12-lts, SSR-6.2.8-lts, SSR-6.3.3-r2 y versiones más recientes.

> *«La vulnerabilidad se ha corregido automáticamente en los dispositivos que operan*

> *con WAN Assurance (donde también se gestiona la configuración) conectados a la nube de Mist. Sin embargo, se recomienda que los routers se actualicen a una versión que contenga la corrección, siempre que sea posible»,* añadió la empresa.