Juniper Networks ha emitido una advertencia sobre una campaña maliciosa que está explotando productos Session Smart Router (SSR) que aún conservan contraseñas predeterminadas para distribuir el malware de la botnet Mirai.

La empresa explicó que lanzó esta alerta luego de que *«varios clientes»* reportaran actividades inusuales en sus plataformas Session Smart Network (SSN) el 11 de diciembre de 2024.

> *«Estos sistemas han sido comprometidos por el malware Mirai, y posteriormente se emplearon como origen de ataques DDoS hacia otros dispositivos accesibles desde su red. Todos los sistemas afectados utilizaban contraseñas predeterminadas»,* afirmó Juniper.

El malware Mirai, cuyo código fuente fue filtrado en 2016, ha dado lugar a múltiples variantes a lo largo del tiempo. Este programa malicioso puede detectar vulnerabilidades conocidas y credenciales predeterminadas para infiltrarse en dispositivos y convertirlos en parte de una botnet que realiza ataques de denegación de servicio distribuido (DDoS).

Para prevenir este tipo de amenazas, se recomienda a las organizaciones:

- Cambiar inmediatamente las contraseñas por unas más robustas y únicas (si aún no lo han hecho).
- Revisar con regularidad los registros de acceso para identificar actividad sospechosa.
- Configurar firewalls para evitar accesos no autorizados.
- Mantener todos los programas y sistemas actualizados.

Entre los signos que podrían indicar un ataque asociado con Mirai se encuentran:

- Escaneo inusual de puertos.
- Intentos reiterados de inicio de sesión por SSH, característicos de ataques de fuerza bruta.

- Aumento repentino del tráfico saliente hacia direcciones IP desconocidas.
- Reinicios inesperados del sistema.
- Conexiones procedentes de direcciones IP maliciosas reconocidas.

> *«Si se descubre que un sistema ha sido infectado, la única forma segura de eliminar la amenaza es reinstalar completamente el sistema, ya que no se puede determinar con precisión qué pudo haberse modificado o extraído del dispositivo»,* explicó la compañía.

Este incidente coincide con un informe reciente del AhnLab Security Intelligence Center (ASEC), que advierte sobre ataques dirigidos a servidores Linux mal configurados, especialmente aquellos con servicios SSH expuestos públicamente. Estos ataques están siendo realizados por un nuevo tipo de malware DDoS conocido como cShell.

> *«cShell está desarrollado en el lenguaje de programación Go y utiliza herramientas de Linux como screen y hping3 para ejecutar ataques DDoS»,* explicó ASEC.