Palo Alto Networks ha informado que ha detectado intentos de acceso por fuerza bruta dirigidos a sus gateways GlobalProtect que usan PAN-OS, pocos días después de que investigadores de amenazas alertaran sobre un aumento en la actividad sospechosa de escaneo de inicios de sesión contra sus dispositivos.

Un vocero de la empresa comentó:

> "*Nuestros equipos están observando indicios de actividades típicas de ataques relacionados con contraseñas, como intentos de acceso por fuerza bruta. No hay indicios de que se esté explotando alguna vulnerabilidad.*"
> Añadió que continúan monitoreando activamente la situación y analizando la actividad detectada para evaluar su impacto y determinar si es necesario aplicar medidas de mitigación.

Este anuncio se produce luego de que la firma de inteligencia de amenazas GreyNoise reportara un aumento significativo en los escaneos de inicio de sesión contra portales GlobalProtect que usan PAN-OS.

Según GreyNoise, esta actividad maliciosa comenzó el 17 de marzo de 2025 y alcanzó un pico con 23,958 direcciones IP únicas involucradas, antes de disminuir hacia finales de ese mes. Todo indica que se trata de un esfuerzo coordinado para probar defensas de red y encontrar sistemas vulnerables o expuestos.

Los escaneos han estado dirigidos principalmente a sistemas ubicados en Estados Unidos, Reino Unido, Irlanda, Rusia y Singapur.

Hasta el momento, se desconoce el alcance total de estas acciones o si están vinculadas a algún grupo específico de amenazas.

Mientras tanto, se recomienda a todos los clientes asegurarse de tener instalada la versión más reciente de PAN-OS. También se aconseja aplicar otras medidas de protección, como:

- Activar la autenticación multifactor (MFA).
- Configurar GlobalProtect para que soporte notificaciones de MFA.
- Establecer políticas de seguridad que detecten y bloqueen intentos de fuerza bruta.
- Limitar la exposición innecesaria de los sistemas a internet.