Boletín de alerta

Boletín Nro.:
Fecha de publicación: 09/06/2026
Tema: Alerta 2026-61 Bypass de Autenticación Activamente Explotado en Check Point
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Check Point Security Gateways

- R82.10 Jumbo Hotfix Take 19 o inferior
- R82 Jumbo Hotfix Take 103 o inferior
- R81.20 Jumbo Hotfix Take 141 o inferior
- R81.10 (EOS)
- R81 (EOS)
- R80.40 (EOS)

Check Point Spark Firewalls

- R80.20.X (EOS)
- R81.10.X
- R82.00.X

Descripción

Check Point ha identificado y confirmado la explotación activa de una vulnerabilidad crítica que afecta a implementaciones de acceso remoto VPN configuradas con el protocolo IKEv1, una tecnología actualmente considerada obsoleta. La falla se origina en un error lógico dentro del proceso de validación de certificados, permitiendo que un atacante remoto no autenticado establezca una sesión VPN válida sin conocer la contraseña de un usuario legítimo. Aunque inicialmente el acceso obtenido corresponde únicamente a la conexión VPN, los atacantes pueden utilizar dicho acceso como punto de entrada para realizar movimientos laterales, reconocimiento interno, robo de información o escalamiento de privilegios. Check Point ha observado ataques reales dirigidos a organizaciones de distintos sectores a nivel mundial y ha vinculado parte de la actividad posterior a la explotación con operadores asociados al ransomware Qilin.

La vulnerabilidad puede ser explotada cuando se cumplen las siguientes condiciones:

- El servicio de Remote Access VPN o Mobile Access está habilitado.
- El protocolo IKEv1 se encuentra habilitado.
- El gateway acepta clientes VPN heredados.
- No se requiere certificado de máquina para establecer la conexión.
- El sistema utiliza una versión vulnerable de Check Point.

Indicadores de Compromiso (IoC)

Direcciones IP observadas durante los ataques

- 45.77.149[.]152
- 209.182.225[.]136
- 38.60.157[.]139
- 162.33.177[.]101
- 45.76.26[.]42
- 144.208.127[.]155
- 38.54.88[.]201
- 38.54.107[.]167
- 66.42.99[.]200
- 45.63.104[.]106
- 45.61.136[.]173

Hashes observados

MD5

- 52fda5c1b9704544f32ee98d9060e689
- 51d39aa39478beeac94f2d12f682ecce

Solución:

- Actualizar todos los Security Gateways y Firewalls afectados con los parches publicados por Check Point.
- Aplicar los últimos Jumbo Hotfix disponibles para cada versión soportada.

Información adicional:

- Vulnerabilidad crítica en parches de la VPN de Check Point (CVE-2026-50751) – Blog de Check Point
- Explotan vulnerabilidad crítica en la VPN de Check Point ~ Segu-Info – Ciberseguridad desde 2000
- NVD – CVE-2026-50751