Vulnerabilidades críticas explotadas en VPN de Check Point

La Unidad de Seguridad TIC, siguiendo las indicaciones marcadas por el SOC de la Junta de Andalucía, avisa de una **campaña de explotación activa asociada a vulnerabilidades en dispositivos de Check Point**, **que afectan al protocolo VPN IKEv1**, permitiendo el acceso no autorizado.

Detalle

La vulnerabilidad principal, explotada en ataques de día cero, identificada como CVE-2026-50751 (puntuación CVSS: 9,3), consiste en una debilidad en el flujo lógico de la validación de certificados que permite a un atacante remoto no autenticado establecer una conexión VPN sin credenciales válidas, debido a un fallo en la lógica de validación de certificados de los módulos Remote Access y Mobile Access.

Para su explotación exitosa, se deben cumplir las siguientes condiciones:

- El acceso remoto VPN o el acceso móvil deben estar habilitados.
- IKEv1 debe estar habilitado para el acceso remoto.
- Los *gateways* deben aceptar clientes de acceso remoto heredados.
- Los *gateways* no deben requerir un certificado de máquina para las conexiones.

Asociada a la vulnerabilidad anterior se ha descubierto una segunda (identificada como CVE-2026-50752) que afecta la validación de certificados en el intercambio de claves IKEv1 obsoleto y que puede ser explotada en ataques de intermediario en conexiones VPN de sitio a sitio.

Detrás de la campaña de explotación se encuentra un actor de amenazas asociado al *ransomware* Qilin.

Recursos Afectados

Los sistemas afectados son:

CVE-2026-50751 (explotada actualmente)

- Check Point Mobile Access / SSL VPN
- Remote Access VPN
- Security Gateways: versiones 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) y R80.40 (EOS)
- Spark Firewalls: Versiones R80.20.X (EOS), R81.10.X y R82.00.X

CVE-2026-50752

- Security Gateways: versiones 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) y R80.40 (EOS)
- Spark Firewalls: Versiones R80.20.X (EOS), R81.10.X y R82.00.X

Recomendaciones Actualizadas (09/06/2026)

Mitigación

1º. Solución a las vulnerabilidades:

Se recomienda actualizar los sistemas siguiendo las indicaciones que proporciona el fabricante:

- https://support.checkpoint.com/results/sk/sk185033
- https://support.checkpoint.com/results/sk/sk185035

2º. *Workaround* a la vulnerabilidad:

En caso de no poder actualizar de forma inmediata, se recomienda aplicar las siguientes medidas de mitigación:

- https://support.checkpoint.com/results/sk/sk185033
- https://support.checkpoint.com/results/sk/sk185035

Debido al riesgo potencial que presentan estas vulnerabilidades, desde la USTIC rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente al fallo indicado.

Referencias

- Aviso de Check Point: https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/amp/
- CVE202650751: https://www.cve.org/CVERecord?id=CVE-2026-50751
- CVE202650752: https://www.cve.org/CVERecord?id=CVE-2026-50752

En caso de haber detectado la explotación de esta vulnerabilidad:

debes reportar el incidente de seguridad con el código USTIC-AV1026, informando en el área personal de ayudaDIGITAL: Asesoramiento vulnerabilidad en seguridad

---

Para cualquier otra duda o consulta al respecto, podéis contactar con ustic.dgtic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Dirección General de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud