e-dea NETWORKS | CYBER SECURITY

BOLETÍN INFORMATIVO

24 - julio – 2026

Vulnerabilidades en Checkpoint

Checkpoint publicó vulnerabilidades que afectan a sus productos.

Estás vulnerabilidades se encuentran asociadas a los CVE-2026-50751 y CVE-2026-50752 de las cuales afectan la validación de certificados en el intercambio de claves IKEv1 obsoleto, puede permitir la interferencia de un atacante intermediario en las comunicaciones VPN de sitio a sitio bajo ciertas condiciones, permite eludir la autenticación del usuario aprovechando una debilidad en el flujo lógico de la validación del certificado de acceso remoto o acceso móvil, y establecer una conexión VPN de acceso remoto sin una contraseña válida.

Hasta la fecha, la explotación de estás vulnerabilidades reportadas, se ha limitado a unas pocas docenas de organizaciones objetivo a nivel mundial. Un caso involucró actividad posterior a la intrusión confirmada asociada con una filial del ransomware Qilin.

Productos **afectados**

CVE	Producto	Versión afectada
CVE-2026-50751	Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall	R80.20.X (EOS), R80.40 (EOS), R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10
CVE-2026-50752	Security Gateways, Spark Firewall	R80.20.X (EOS), R80.40 (EOS), R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10

Recomendaciones

CVE-2026-50751



Severidad: **Crítica**
CVSS: **9.3**

Parches

Actualizar a las versiones corregidas indicadas por el fabricante y validar la documentación.

CVE-2026-50752



Severidad: **Alta**
CVSS: **7.4**

Configuración

- *Eliminar la compatibilidad con el cliente de acceso remoto heredado.*
- *Configurar las propiedades globales para la autenticación VPN de acceso remoto solo para IKEv2.*
- *Establecer la autenticación mediante certificado como obligatorio.*

Fuentes: *Checkpoint support ID sk185033* *Checkpoint support ID sk185035* ,