Boletín de alerta

Boletín Nro.:
Fecha de publicación: 23/07/2026
Tema: Alerta 2026-76 Check Point Corrige Vulnerabilidades con Explotación Activa
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Check Point Security Management**: R81.10, R81.20, R82, R82.10 y versiones anteriores.
- **Check Point Multi-Domain Management (MDM)**: R81.10, R81.20, R82, R82.10 y versiones anteriores.
- **Check Point GaiaOS Web Interface**: R81.10, R81.20, R82, R82.10 y versiones anteriores.

Descripción

Check Point publicó una actualización de seguridad urgente para corregir tres vulnerabilidades críticas identificadas durante su programa de revisión de seguridad BLAST. La más grave, **CVE-2026-16232 (CVSS 9.3)**, está siendo explotada activamente y permite a un atacante remoto no autenticado obtener acceso administrativo mediante la evasión del proceso de autenticación de SmartConsole. La explotación se ha observado principalmente en entornos donde las interfaces de administración están expuestas directamente a Internet sin restricciones de acceso por dirección IP. Una vez comprometido el sistema, un atacante puede modificar políticas de seguridad, crear cuentas privilegiadas, alterar configuraciones y comprometer la infraestructura administrada.

CVE-2026-62144 – Bypass de autenticación y escalada de privilegios (CVSS 9.3)

La vulnerabilidad **CVE-2026-62144** afecta a **Check Point Security Management** y **Multi-Domain Management**, permitiendo que un atacante eluda los mecanismos de autenticación y obtenga privilegios elevados sobre la plataforma de administración

CVE-2026-62145 – Escalada local de privilegios en GaiaOS (CVSS 7.5)

La vulnerabilidad **CVE-2026-62145** afecta a la interfaz web de **GaiaOS** y permite que un usuario con acceso local incremente sus privilegios dentro del sistema.

IOC

Direcciones IP observadas:
151.241.99[.]207

151.241.99[.]233
158.62.198[.]182
192.142.10[.]99
139.28.37[.]250
194.213.18[.]137

Solución:

Se recomienda implementar las siguientes acciones de forma inmediata:

- Instalar el **Jumbo Hotfix** publicado por Check Point el **22 de julio de 2026**.
- Restringir el acceso a las interfaces de administración únicamente desde direcciones IP o subredes de confianza.
- Evitar que las interfaces de administración estén expuestas directamente a Internet.

Información adicional:

- Known Exploited Vulnerabilities Catalog | CISA
- Security Advisory – Action Required – July 2026 Security Update – Check Point Blog
- CISA Warns of Check Point Authentication Vulnerability Exploited in Attacks