

Boletín de alerta

Boletín Nro.: 103

Fecha de publicación: 18/09/2026

Tema: Alerta 2026-103 Vulnerabilidad RCE crítica como root en Check Point Security Management y Log Servers

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto / componente	Estado
Check Point Security Management Server	Afectado
Check Point Multi-Domain Security Management Server	Afectado
Check Point Log Server	Afectado
Check Point Multi-Domain Log Server	Afectado
Despliegues Standalone (Management + Gateway en el mismo equipo)	Afectado
Smart-1 Cloud	No afectado; la corrección ya fue desplegada por Check Point

Un servidor se considera vulnerable si ejecuta cualquiera de las siguientes ramas con el **Jumbo Hotfix Take** indicado o una versión anterior:

Rama	Rango afectado	Corrección recomendada
R82.20	Todas las builds	Instalar el <i>LivePatch</i> / actualización urgente disponible para R82.20
R82.10	Jumbo Hotfix Take 44 o anterior	Instalar el <i>LivePatch</i> o actualizar a un Take posterior corregido
R82	Jumbo Hotfix Take 126 o anterior	Instalar el <i>LivePatch</i> o actualizar a un Take posterior corregido
R81.20	Jumbo Hotfix Take 166 o anterior	Instalar el <i>LivePatch</i> o actualizar a un Take posterior corregido
R81.10	Jumbo Hotfix Take 190 o anterior	Rama EoS; solicitar fix a Check Point Support o planificar migración prioritaria

Descripción

Se ha publicado una vulnerabilidad en Check Point, etiquetada como **CVE-2026-91843**, una vulnerabilidad crítica de tipo *stack-based buffer overflow* en el proceso de inicio de sesión de sus servidores de administración y registro. La falla tiene una puntuación **CVSS 9.8** y puede permitir que un atacante remoto no autenticado ejecute código arbitrario con privilegios **root**.

CVE-2026-91843 es una vulnerabilidad de desbordamiento de búfer basado en pila, clasificada como **CWE-121**, en el proceso de login de Security Management Server y Log Server. La condición vulnerable ocurre **antes de la autenticación**: un atacante remoto puede enviar una solicitud de inicio de sesión con un nombre de usuario excesivamente largo y provocar el desbordamiento.

La ruta vulnerable se encuentra asociada al mecanismo de **Trusted Clients**, que define qué equipos pueden conectarse al servidor de administración mediante SmartConsole. Según Check Point, la vulnerabilidad es alcanzable únicamente a través de esta configuración de clientes confiables. Una configuración permisiva, especialmente si usa el valor **"Any"** o permite acceso desde Internet, incrementa significativamente la superficie de ataque.

Un compromiso exitoso de un Management Server es especialmente grave porque este componente controla políticas de seguridad, configuración de gateways, objetos de red, credenciales y acceso administrativo del ecosistema Check Point. La ejecución como root podría permitir modificar políticas de firewall, introducir reglas de acceso no autorizadas, alterar registros, extraer configuraciones y utilizar el servidor como punto de pivote hacia gateways y otros activos administrados.

El fabricante recomienda aplicar de inmediato la corrección mediante **Check Point LivePatch** o el paquete de actualización offline correspondiente. Al momento de la publicación, Check Point indicó que no tenía evidencia de explotación activa y CISA registraba el estado de explotación como "none"; sin embargo, por tratarse de una falla preautenticación, remota y con ejecución como root en la infraestructura de gestión, la remediación debe considerarse de máxima prioridad.

Solución

La solución principal es aplicar el *LivePatch* indicado en el advisory **sk1000155**. Los equipos con actualizaciones automáticas habilitadas conforme a la configuración de Check Point pueden recibir la corrección automáticamente, pero los administradores deben verificar su instalación mediante *cplp list*.

<https://support.checkpoint.com/results/sk/sk1000155>

Para entornos sin LivePatch o sin actualizaciones automáticas, Check Point proporciona paquetes de actualización urgente offline. Se reportan paquetes **Take 29** para R82.20 y **Take 28** para R82.10, R82 y R81.20; confirmar el paquete exacto aplicable desde el portal de soporte y el advisory antes de desplegarlo.

No existe una mitigación que reemplace la aplicación del parche. La restricción de Trusted Clients, la eliminación de "Any" y el cierre de acceso directo a Internet son controles compensatorios importantes, pero el *LivePatch* debe instalarse de forma prioritaria.

Información adicional:

- <https://support.checkpoint.com/results/sk/sk1000155>
- <https://www.cve.org/CVERecord?id=CVE-2026-91843>
- <https://thehackernews.com/2026/09/critical-check-point-management-server.html>