Una vulnerabilidad crítica en los Security Management Servers y Log Servers de Check Point podría permitir que un atacante sin credenciales válidas ejecute código con privilegios de *root* de forma remota a través de la red.

El Security Management Server es el componente encargado de administrar las políticas de firewall y gestionar el acceso de los administradores. Check Point publicó una corrección mediante su canal de actualizaciones LivePatch y afirmó que, hasta el momento, no tiene evidencia de que la vulnerabilidad haya sido explotada.

Check Point informó que la ruta vulnerable solo puede explotarse a través de la configuración Trusted Clients, la cual determina qué equipos pueden conectarse al servidor de administración mediante SmartConsole.

La vulnerabilidad, identificada como CVE-2026-91843 y calificada con una puntuación de 9.8 sobre 10 en la escala CVSS por Check Point, consiste en un desbordamiento de pila (*stack overflow*) dentro del proceso de autenticación. Este componente procesa solicitudes antes de que el usuario complete la autenticación. La empresa de análisis de Internet Censys indicó que el fallo puede activarse mediante una solicitud de inicio de sesión que contenga un nombre de usuario excesivamente largo.

En un aviso publicado el 16 de septiembre de 2026 en la comunidad CheckMates, Check Point señaló que los clientes con actualizaciones automáticas habilitadas ya están protegidos. Para los demás usuarios, recomendó instalar inmediatamente la corrección distribuida mediante LivePatch y detallada en el boletín sk1000155. Asimismo, instó a actuar con urgencia debido a la gravedad del fallo y al posible impacto sobre los sistemas afectados.

“Por el momento, no existe ninguna evidencia de que esta vulnerabilidad haya sido explotada en entornos reales.”

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) también registró el estado de explotación como *“ninguna”* en la evaluación adjunta al registro CVE el 17 de septiembre.

La vulnerabilidad tampoco figuraba en el catálogo de Known Exploited Vulnerabilities de CISA en su actualización del 16 de septiembre. Por su parte, Censys indicó que no existía una prueba de concepto pública (*Proof of Concept – PoC*) al 16 de septiembre. Aviv Abramovich, vicepresidente de gestión de productos de seguridad de red en Check Point, confirmó a *The Hacker News* que la compañía no había recibido reportes de explotación.

Versiones afectadas

El registro CVE de Check Point identifica las siguientes ramas afectadas según la versión de Jumbo Hotfix Take, el paquete acumulativo de correcciones utilizado por cada versión del producto.

Cualquier servidor que ejecute una de las siguientes ramas con la versión indicada o una anterior se considera vulnerable:

- R82.10 con Jumbo Hotfix Take 44 o inferior.
- R82 con Jumbo Hotfix Take 126 o inferior.
- R81.20 con Jumbo Hotfix Take 166 o inferior.
- R81.10 con Jumbo Hotfix Take 190 o inferior.
- R81, R80.40, R80.30, R80.20, R80.10 y R80, todas ellas actualmente fuera de soporte.

Aunque el registro CVE no incluye explícitamente la rama R82.20, Abramovich confirmó que también es vulnerable. Según el aviso de Censys, todas las compilaciones de R82.20 presentan el problema y aún no existe un Jumbo Hotfix disponible para proteger dicha versión.

Además, Abramovich indicó que también se ven afectados:

- Despliegues Standalone (administración y gateway en el mismo sistema).
- Log Servers.
- Multi-Domain Servers.

Una alerta emitida por NHS England Digital, basada en la información de sk1000155, señala que el servicio administrado Smart-1 Cloud no se encuentra afectado debido a que ya incorpora la corrección correspondiente.

El registro CVE marca a R81.10 y las versiones anteriores como productos fuera de soporte. Sin embargo, Abramovich indicó que Check Point dispone de una solución para dichas versiones y que los clientes interesados deben solicitarla mediante un ticket al soporte técnico.

Recomendaciones para administradores

Los administradores deberían adoptar las siguientes medidas:

1. Aplicar la corrección LivePatch descrita en el boletín sk1000155 en todos los Security Management Servers y Log Servers.
2. Si las actualizaciones automáticas están habilitadas, verificar que la corrección efectivamente se haya instalado. El comando cplp list permite revisar los LivePatches aplicados y su estado actual.
3. Independientemente de que el parche esté instalado o no, revisar que la configuración Trusted Clients esté restringida únicamente a equipos confiables y conocidos. Asimismo, evitar que el acceso de administración quede expuesto directamente a Internet.

El término *"actualizaciones automáticas"* hace referencia a la configuración descrita en sk175504. Esta opción se encuentra en SmartConsole, dentro de Global Properties → Data Access Control, mediante la casilla:

"Automatically download and install Software Blade Contracts, security updates, and other important data (highly recommended)."

Tras habilitarla, debe instalarse la política de Access Control. El mecanismo LivePatch es utilizado por Check Point para distribuir correcciones urgentes de seguridad a los sistemas

que tengan activada esta función.

Es importante considerar que la distribución de actualizaciones no siempre ocurre de manera inmediata. La semana anterior, durante la publicación de los parches para dos vulnerabilidades relacionadas con certificados VPN, varios clientes informaron en la comunidad de Check Point que aún no habían recibido automáticamente los paquetes de actualización el mismo día del anuncio. Un administrador de la comunidad respondió que el despliegue probablemente se realizaba por fases y no simultáneamente para todos los usuarios.

Los usuarios también reportaron que los enlaces de descarga incluidos en esos avisos solo estaban disponibles después de iniciar sesión en el portal User Center.

Configuración Trusted Clients

Según la guía de endurecimiento (*hardening guide*) de Check Point, la configuración Trusted Clients puede encontrarse en:

Manage & Settings → Permissions & Administrators → Trusted Clients

La misma guía recomienda evitar el acceso directo a la consola de administración desde Internet y exige el uso de una VPN. Abramovich reiteró que la vulnerabilidad solo puede explotarse a través de la funcionalidad Trusted Clients y que los clientes deben asegurarse de que esta configuración no permita el acceso desde cualquier dirección IP, sino únicamente desde sistemas de confianza.

Exposición en Internet

Censys informó haber identificado 3,836 hosts a nivel mundial que muestran la identidad predeterminada asignada por Check Point a sus servidores de administración y registros. La compañía eligió este método de medición porque el nivel exacto de compilación y de parches instalados no puede determinarse mediante escaneo remoto.

“Esta cifra representa la presencia total de estos roles y no un conteo confirmado de sistemas vulnerables.”

Quinta vulnerabilidad crítica de gestión desde julio

De acuerdo con el análisis realizado por *The Hacker News* sobre los registros CVE de Check Point, CVE-2026-91843 constituye la quinta vulnerabilidad crítica descubierta desde el 22 de julio que podría ser explotada contra un Security Management Server sin necesidad de autenticación previa.

La primera fue CVE-2026-16232, una vulnerabilidad de omisión de autenticación (*authentication bypass*) en SmartConsole que fue explotada durante julio. En aquel momento, Lotem Finkelstein, de Check Point, indicó que el incidente afectó:

“a un reducido número de clientes”

en una configuración específica,

“cuando el Management estaba expuesto directamente a Internet sin restricciones de direcciones IP.”

La principal medida de mitigación recomendada entonces coincide con la actual: limitar la lista de Trusted Clients exclusivamente a direcciones de confianza.

Ese mismo día, CISA incorporó CVE-2026-16232 en su catálogo de vulnerabilidades explotadas activamente. No obstante, otra vulnerabilidad de bypass de administración divulgada simultáneamente, CVE-2026-62144, no fue reportada como explotada.

Posteriormente se revelaron dos vulnerabilidades adicionales:

- CVE-2026-18574, divulgada el 3 de agosto, que permitía la omisión de autenticación y potencial ejecución de comandos en el servidor de administración.

- CVE-2026-85103, publicada el 9 de septiembre, relacionada con un desbordamiento de memoria (*heap overflow*) durante la decodificación de certificados VPN, afectando también a Quantum Security Management.

Check Point afirmó haber identificado internamente ambas vulnerabilidades y no contar con evidencias de explotación.

Hasta el momento, no se ha revelado quién descubrió CVE-2026-91843, y Check Point no respondió a las consultas sobre ese aspecto.