# Boletín informativo vulnerabilidades de Apex One

**CSIRTSALUD-AL-20250808-13** **TLP: CLEAR**

| | |
|---|---|
| **Incidente ID:** | 0013 |
| **Fecha del reporte:** | 08/08/2025 |
| **Entidad:** | Todas las entidades del ecosistema digital |
| **Título:** | Vulnerabilidades críticas de Apex One Management console |
| **Herramienta de detección** | TrendMicro |
| **Activo involucrado:** | Consola de gestión local de Trend Micro Apex One (on-premise) |
| **Tipo de incidente:** | Boletín informativo |
| **Nivel de riesgo:** | Crítico |

## Objetivo:

Informar a las entidades del Ecosistema Digital sobre las vulnerabilidades críticas en las versiones locales de Apex One Management Console.

## Descripción:

Las vulnerabilidades ( **CVE-2025-54948** y **CVE-2025-54987** ), ambas calificadas con 9,4 en el sistema de puntuación CVSS, han sido descritas como fallas de inyección de comandos en la consola de administración y ejecución remota de código.

# Boletín informativo vulnerabilidades de Apex One

**CSIRTSALUD-AL-20250808-13** **TLP: CLEAR**

Una vulnerabilidad en la consola de administración local de Trend Micro Apex One podría permitir que un atacante remoto previamente autenticado cargue código malicioso y ejecute comandos en las instalaciones afectadas

Si bien ambas deficiencias son esencialmente las mismas, la CVE-2025-54987 afecta a una arquitectura de CPU diferente. El equipo de Respuesta a Incidentes (IR) de Trend Micro y Jacky Hsieh, de CoreCloud Tech, han sido responsables de informar sobre ambas fallas.

**Para explotar este tipo de vulnerabilidades**, generalmente se requiere que un atacante tenga acceso (físico o remoto) a una máquina vulnerable.

## Impacto:

Ejecución remota de código (RCE) sin necesidad de autenticación previa, exfiltración de datos, ejecución de comandos arbitrarios, y posible escalada de privilegios en sistemas empresariales.

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Vulnerabilidad:** CVE-2025-54948 y CVE-2025-54987

**Puntuación base**: 9.4

**Gravedad**: Crítica

**Herramienta de detección**: Aplicación de la herramienta temporal (“fix tool”) publicada por Trend Micro como mitigación inmediata.

## Productos afectados:

**Trend Micro Apex One (on-premise)**

- Consola de gestión local (no afecta a la versión en la nube o SaaS).
- Vulnerabilidades explotadas en el componente web de administración.
- Versiones afectadas: anteriores a la actualización de agosto de 2025

**Trend Micro Apex One as a Service**

- **No está afectado** directamente, según la información actual, ya que el entorno es gestionado por Trend Micro con parches aplicados automáticamente.

## Recomendaciones de mitigación:

**Pasos de Remediación Urgente**

1. **Aplicar la herramienta de mitigación temporal (fix tool)**

   Trend Micro ha liberado una herramienta oficial para mitigar de forma inmediata las vulnerabilidades mientras se publica el parche definitivo, a continuación, se comparte el link de descarga

   - https://success.trendmicro.com/en-US/solution/KA-0009781?utm_source

2. **Restringir el acceso a la consola de administración**

   - Validar que la consola web de Apex One no sea accesible públicamente desde Internet. Es preferible que toda la administración se realice de manera interna.
   - Si el acceso a la consola se realiza de manera externa o si se tiene expuesta en una red interna a equipos que podrían no estar autorizados, se recomienda limitar el acceso por red (firewall o ACLs) solo a direcciones IP internas y autorizadas.

3. **Monitorear actividad sospechosa**

   - Realizar un monitoreo de los logs de la consola de Apex One en busca de accesos no autorizados o comportamiento anómalo.

- Corroborar con otras herramientas tales como SIEM u otra solución de monitoreo para detectar posibles intentos adicionales de explotación.

4. **Actualizar el producto tan pronto como esté disponible el parche oficial**

- Trend Micro ha confirmado que el parche completo será liberado próximamente a mediados de Agosto. Por lo que las Entidades deben implementar la actualización de inmediato.
- Se recomienda suscribirse a alertas del portal de seguridad de Trend Micro para recibir notificaciones inmediatas.

## Recomendaciones adicionales:

- Habilitar la funcionalidad de multifactor (MFA) para controlar el acceso a la consola de administración y añadir una capa extra de seguridad.
- Asignar los roles y permisos mínimos que sean necesarios a los usuarios que acceden a la consola para reducir el riesgo de abuso o errores.
- Implementar la segmentación adecuada de red para separar los servidores de gestión de endpoints de otros sistemas críticos.
- Informar y capacitar al personal responsable sobre las vulnerabilidades, su impacto y las acciones preventivas.

## Fuentes:

- https://success.trendmicro.com/en-US/solution/KA-0009781?utm_source
- https://thehackernews.com/2025/08/trend-micro-confirms-active.html
- https://success.trendmicro.com/en-US/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.