Alerta Id	0018
Fecha del reporte	08/20/2025
Entidad	Todas las entidades del ecosistema digital
Título	Vulnerabilidad crítica en Trend Micro Apex One Management Console (CVE-2025-54948)
Herramienta de detección	Fortirecon
Activo involucrado	Trend Micro Apex One Management Console (on-premise)
Tipo de alerta	Vulnerabilidad crítica (Inyección de comandos – CWE-78)
Nivel de riesgo	Alto

Objetivo

Informar a las entidades del ecosistema digital sobre la **explotación activa de la vulnerabilidad CVE-2025-54948 en Trend Micro Apex One Management Console (on-premise)**.

La explotación de esta falla crítica permite a un atacante remoto, con autenticación previa o credenciales obtenidas mediante otras técnicas, **inyectar y ejecutar comandos arbitrarios del sistema operativo**, comprometiendo por completo los servidores afectados.

El objetivo de la alerta es que las organizaciones:

- **Identifiquen de inmediato** si cuentan con instancias vulnerables de Apex One.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **Implementen medidas de mitigación urgentes**, incluyendo parches y controles de seguridad adicionales.
- **Prevean escenarios de ataque avanzados**, como despliegue de ransomware, persistencia de atacantes y exfiltración de datos sensibles.
- **Refuercen sus capacidades de monitoreo y respuesta a incidentes** en torno a esta vulnerabilidad.

Descripción

La vulnerabilidad **CVE-2025-54948** se encuentra en la **consola de administración on-premise de Trend Micro Apex One**, una de las plataformas de seguridad empresarial más utilizadas en el sector corporativo y gubernamental.

El fallo está catalogado bajo **CWE-78 (Neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo)** y se debe a una **validación insuficiente de entradas en la interfaz de administración**, lo que permite a atacantes inyectar comandos maliciosos en solicitudes especialmente diseñadas.

CISA confirmó el **18 de agosto de 2025** que la vulnerabilidad ya está siendo **explotada activamente** en entornos reales, incorporándose a su **Known Exploited Vulnerabilities Catalog (KEV)**. Esto activa obligaciones de remediación bajo la **Binding Operational Directive (BOD) 22-01** para agencias del gobierno federal de EE.UU., con fecha límite de **8 de septiembre de 2025**.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

De acuerdo con la telemetría de **FortiRecon**, esta vulnerabilidad también está siendo identificada en múltiples escaneos de infraestructura, lo que confirma un **alto interés de los atacantes** en explotarla.

Si bien aún no se ha vinculado oficialmente con campañas de ransomware, su criticidad y el tipo de acceso que otorga la hacen un vector **altamente atractivo para operadores de ransomware y APTs**.

Impacto

La explotación de **CVE-2025-54948** puede generar las siguientes consecuencias:

- **Compromiso total del sistema afectado** mediante ejecución de comandos arbitrarios.
- **Escalación de privilegios** que otorgan al atacante control completo sobre el servidor.
- **Persistencia** dentro de la infraestructura comprometida mediante la manipulación de procesos legítimos.
- **Movimiento lateral** hacia otros sistemas críticos de la red corporativa.
- Posible **despliegue de ransomware**, con impacto en la **continuidad del negocio**, cifrado de archivos, interrupción de servicios críticos y riesgo de **filtración de datos confidenciales**.
- Riesgo de **inhabilitación de controles de seguridad existentes**, dado que Apex One es una plataforma de defensa empresarial, lo que aumenta la superficie de ataque en la

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

organización.

Sectores con mayor exposición potencial:

- **Tecnologías de la Información (TI)**: plataformas empresariales, proveedores de servicios en la nube.
- **Financiero**: entidades bancarias, fintech y aseguradoras.
- **Salud**: hospitales, aseguradoras EPS, clínicas privadas y entes reguladores.
- **Retail y logística**: plataformas con alto volumen transaccional y sistemas críticos de distribución.
- **Bienes raíces y sector público**: uso de Trend Micro en entornos gubernamentales y corporativos.

Recomendaciones de mitigación

Para mitigar los riesgos asociados a **CVE-2025-54948**, se recomienda:

1. **Aplicación inmediata de parches**
    - Implementar las actualizaciones de seguridad publicadas por **Trend Micro** en sus canales oficiales.
    - Si el parche no se encuentra disponible, **suspender temporalmente el uso del producto afectado** en entornos críticos.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

2. **Fortalecimiento de la seguridad perimetral y segmentación**
    - Restringir el acceso a la consola de administración únicamente desde redes internas confiables.
    - Aplicar **controles de segmentación de red** para limitar el movimiento lateral.
3. **Monitoreo y detección temprana**
    - Vigilar intentos de **ejecución de comandos inusuales** o tráfico anómalo asociado a Apex One.
    - Analizar eventos relacionados con intentos de autenticación sospechosos o repetitivos.
    - Implementar reglas de detección en **SIEM/EDR** para identificar uso indebido de procesos legítimos.
4. **Políticas de mínimo privilegio y hardening**
    - Restringir cuentas con privilegios elevados en servidores que ejecutan Apex One.
    - Revisar accesos administrativos y deshabilitar cuentas innecesarias.
5. **Resiliencia operativa y continuidad**
    - Mantener **respaldos cifrados y desconectados de la red de producción**, probando periódicamente la restauración.
    - Implementar planes de contingencia para minimizar la interrupción de servicios en caso de explotación exitosa.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

6. **Concientización y capacitación**

    - Informar a equipos de TI y SOC sobre la criticidad de la vulnerabilidad.

    - Capacitar a los usuarios sobre buenas prácticas de gestión de contraseñas y riesgos de ingeniería social que pueden facilitar el acceso inicial a la consola.

Fuentes

- https://gbhackers.com/cisa-alerts-on-trend-micro-apex-one-vulnerability/
- https://cybersecuritynews.com/cisa-warns-trend-micro-apex-one-flaw/

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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570