Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

TREND MICRO APEX ONE (ON-PREMISE) AFECTADO POR VULNERABILIDADES RCE

12/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente Trend Micro detectó 2 vulnerabilidades de severidad crítica que permiten la inyección de comando (RCE) en la consola de administración de Apex One on-premise, estas han sido identificadas como: CVE-2025-54948 y CVE-2025-54987 se les colocó una criticidad de: CVSS: 9.4.

TREND MICRO APEX ONE (ON-PREMISE) AFECTADO POR VULNERABILIDADES RCE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente Trend Micro detectó 2 vulnerabilidades de severidad crítica que permiten la inyección de comando (RCE) en la consola de administración de Apex One on-premise.

Estas han sido identificadas como: CVE-2025-54948 y CVE-2025-54987 se les colocó una criticidad de: CVSS: 9.4.

¿Cómo funcionan?

1. En un escenario ficticio el atacante accede a la interfaz de administración de Apex One puede ser por red o físicamente.
2. El atacante envía una entrada maliciosa a la consola, diseñada previamente para ejecutarse como comando del sistema operativo.
3. Luego la consola no logra sanitizar de manera correcta la petición, por lo cual pasa directamente al sistema operativo, ejecutando así código arbitrario con los permisos del proceso como el usuario IUSR.
4. En este punto el atacante obtiene permisos para realizar acciones como exfiltrar datos o comprometer el servidor al igual que puede moverse lateralmente dentro de la red.

Diferencias notables entre las vulnerabilidades

Hay una diferencia notable entre estas dos vulnerabilidades y esta radica directamente en la arquitectura de CPU afectada.

- CVE-2025-54948 se aplica a una arquitectura específica.
- CVE-2025-54987 es prácticamente idéntica, pero explotable en otra arquitectura diferente.

¿Qué versiones están afectadas?

Estas vulnerabilidades afectan las versiones 2019 de Apex One Management Server 14039 y anteriores esto para sistemas Windows.

Investigadores han observado al menos un intento activo de explotación en entorno reales.
Las variantes “Apex One as a Service” y “Trend Vision One Endpoint Security” ya cuentan con mitigaciones realizadas desde el 31 de julio de 2025.

RECOMENDACIONES

- Instalar el FixTool_Aug2025 publicado por Trend Micro para mitigar la explotación.
- Verificar la integridad del archivo descargado comparando el hash SHA-256 provisto por Trend Micro.
- Limitar el acceso a la consola web únicamente a direcciones IP internas o de confianza.
- Bloquear el acceso desde internet, utilizando firewalls o reglas de ACL.
- Una vez disponible el parche formal a mediados de agosto 2025, aplicarlo para restaurar funciones y eliminar la vulnerabilidad de raíz.

NOTICIA COMPLETA

https://devel.group/blog/trend-micro-apex-one-on-premise-afectado-por-vulnerabilidades-rce/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group