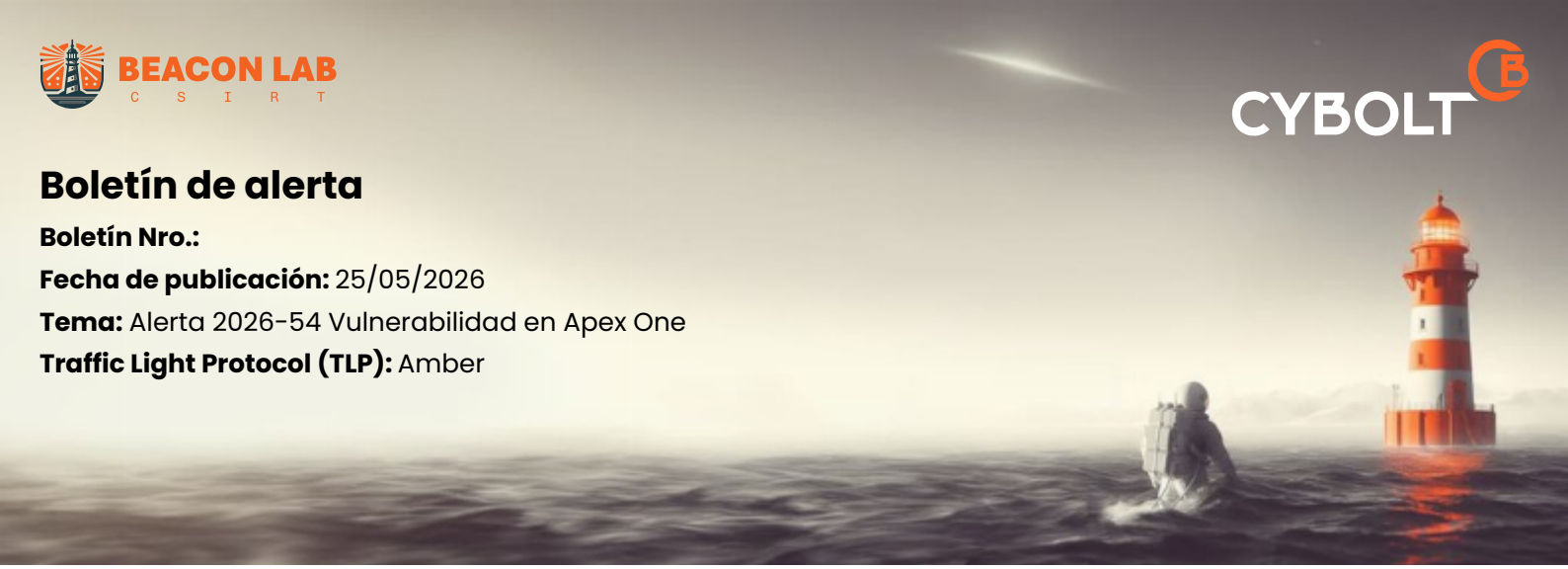

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/05/2026
Tema: Alerta 2026-54 Vulnerabilidad en Apex One
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Trend Micro Apex One (On-Premise)
- Trend Micro Apex One as a Service
- Trend Vision One – Standard Endpoint Protection (SEP)

Descripción

Trend Micro publicó actualizaciones de seguridad para corregir la vulnerabilidad en Apex One y Vision One SEP, destacando la vulnerabilidad CVE-2026-34926, una falla de tipo Directory Traversal que podría permitir a un atacante modificar tablas críticas del servidor e inyectar código malicioso hacia los agentes administrados.

La vulnerabilidad afecta principalmente implementaciones on-premise de Apex One. Un atacante con acceso previo al servidor y credenciales administrativas comprometidas podría modificar configuraciones internas del servidor de administración para distribuir código malicioso automáticamente a los endpoints conectados.

Trend Micro confirmó actividad de explotación en entornos reales y organismos como CISA añadieron la vulnerabilidad al catálogo de Known Exploited Vulnerabilities (KEV) debido a evidencia de explotación activa.

Los investigadores destacan que el riesgo operativo es elevado debido a que Apex One actúa como plataforma centralizada de administración de seguridad, permitiendo propagación de cambios a múltiples sistemas Windows corporativos.

Solución:

Se recomiendan la siguientes acciones de forma inmediata:

- Actualizar Apex One On-Premise a SP1 CP Build 18012 o superior.
- Actualizar agentes de Apex One as a Service / Vision One SEP a Build 14.0.20731 o superior.

Información adicional:

- CVE-2026-34926 – CVE.org
- Trend Micro Security Bulletin
- NVD – CVE-2026-34926
- Cyber Centre Advisory AV26-494