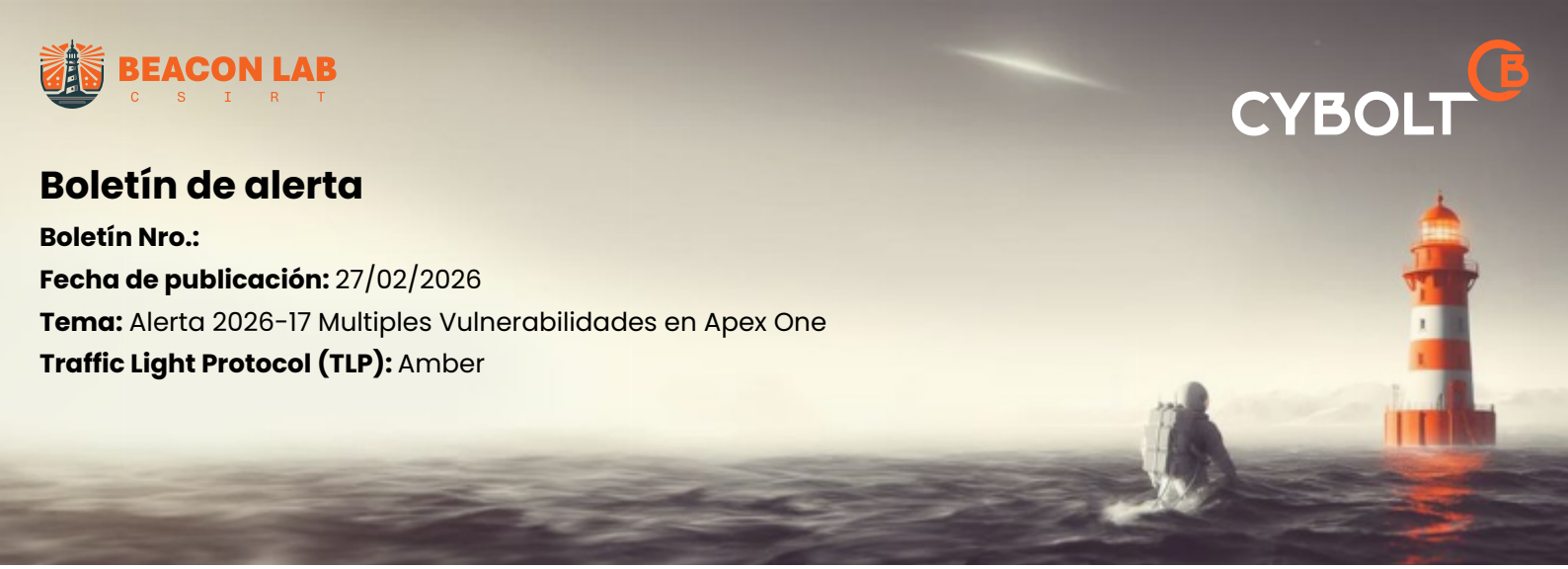

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 27/02/2026
Tema: Alerta 2026-17 Multiples Vulnerabilidades en Apex One
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Tren Micro Apex One

Descripción

Trend Micro ha parcheado dos vulnerabilidades críticas de Apex One que permiten a los atacantes sin privilegios obtener ejecución remota de código (RCE) en sistemas Windows vulnerables.

Ambas vulnerabilidades afectan a la consola de administración de Trend Micro Apex One y podrían permitir que un atacante remoto sin privilegios cargue código malicioso y ejecute comandos en las instalaciones afectadas.

CVE-2025-71210 (CVSS 9.8) es una debilidad en la ruta de acceso en la consola de administración de Trend Micro Apex One, que permite a atacantes sin privilegios ejecutar código malicioso en sistemas sin parches. CVE-2025-71211 es otra vulnerabilidad de en la consola de administración de Apex One, similar en alcance a CVE-2025-71210 (CVSS 9.8) pero que afecta a un ejecutable diferente.

La explotación exitosa requiere que los atacantes tengan acceso a la consola de administración Trend Micro Apex One,

Mitigaciones y soluciones

Los usuarios afectados deben realizar las siguientes acciones:

- Aplicar restricciones de IP de origen
- Descargar las actualizaciones del Centro de descargas de Trend Micro
- Revisar politicas de acceso remoto

Información adicional:

- https://www.bleepingcomputer.com/news/security/trend-micro-warns-of-critical-apex-one-rce-vulnerabilities/
- https://securityaffairs.com/188572/security/trend-micro-fixes-two-critical-flaws-in-apex-one.html
- https://cyberpress.org/critical-trend-micro-apex-one-flaws/