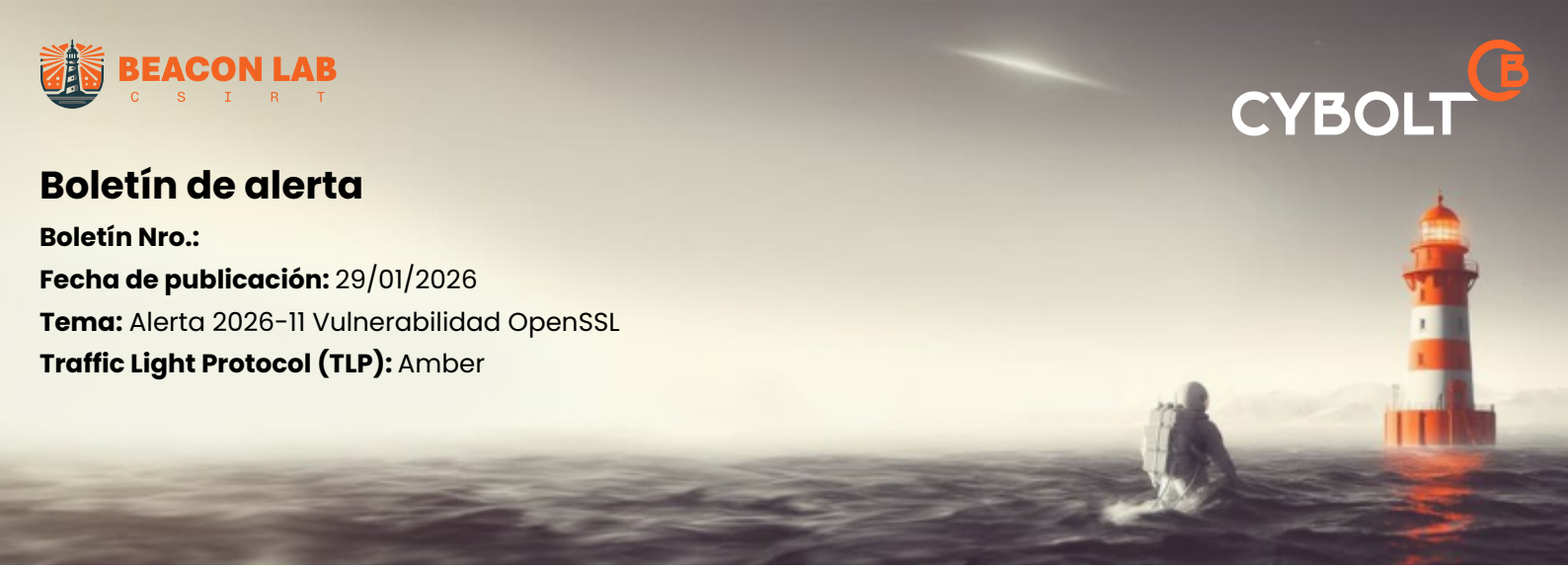

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 29/01/2026
Tema: Alerta 2026-11 Vulnerabilidad OpenSSL
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

• OpenSSL versions 3.6, 3.5, 3.4, 3.3, 3.0

Descripción

Una vulnerabilidad de alta criticidad catalogada como CVE-2025-15467, mediante un desbordamiento del búfer en la pila podría provocar un DoS o ejecución remota de código en determinadas condiciones.

El error reside en la forma en que OpenSSL procesa mensajes específicos de la Sintaxis de Mensajes Criptográficos (CMS), particularmente aquellos que utilizan la estructura AuthEnvelopedData con algoritmos de cifrado AEAD (como AES-GCM).

Al analizar estos mensajes, OpenSSL extrae un dato llamado **Vector de Inicialización (IV)** y lo copia en un espacio de memoria de tamaño fijo sin verificar si el dato es demasiado grande para dicho espacio. Un atacante puede enviar un mensaje diseñado maliciosamente con un IV sobredimensionado, provocando una escritura fuera de los límites de la memoria.

Solución

Los usuarios afectados deben actualizar a las siguientes versiones:

- 3.6 ⊠3.6.1
- 3.5 ⊠3.5.5
- 3.4 ⊠3.4.4
- 3.3 ⊠3.3.6
- 3.0 ⊠3.0.19

Información adicional:

- https://research.jfrog.com/post/potential-rce-vulnerabilityin-openssl-cve-2025-15467/
- https://access.redhat.com/security/cve/cve-2025-15467
- https://nvd.nist.gov/vuln/detail/CVE-2025-15467
- https://cyberpress.org/openssl-vulnerabilities-remote-execute-malicious-code/