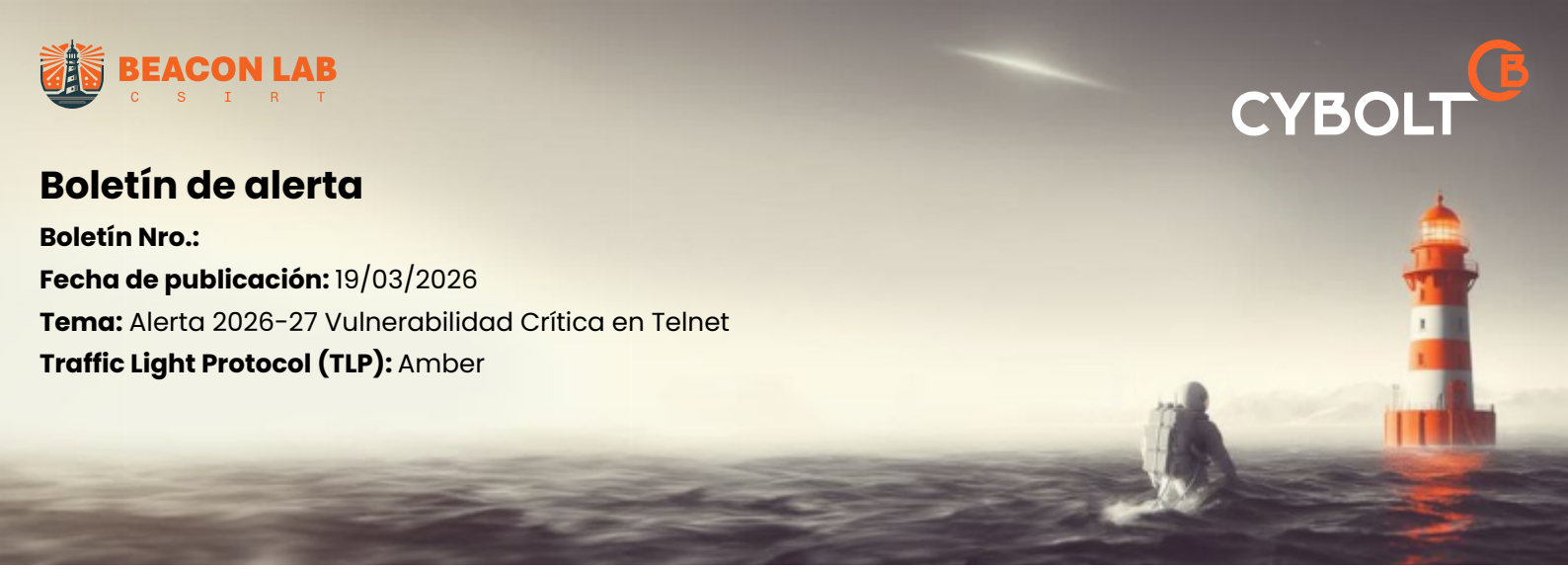


Boletín de alerta

Boletín Nro.:
Fecha de publicación: 19/03/2026
Tema: Alerta 2026-27 Vulnerabilidad Crítica en Telnet
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- GNU Inetutils (servicio telnetd)
- Versiones afectadas: todas hasta la versión 2.7
- Impacta sistemas Linux, dispositivos IoT y entornos OT/ICS que utilicen Telnet

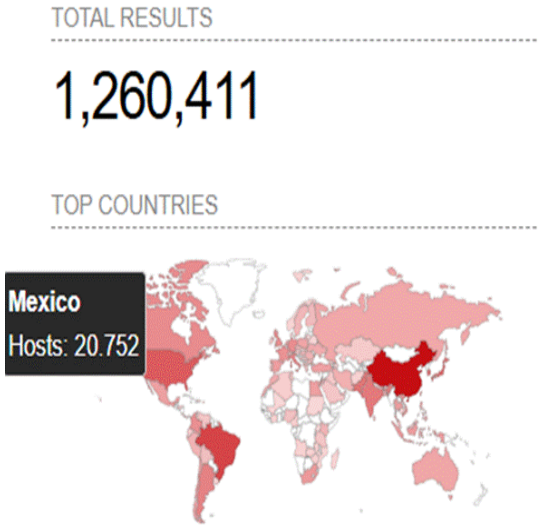
Descripción

Se identificó la vulnerabilidad **CVE-2026-32746** con una puntuación **CVSS 9.8 (Crítica)**. La falla afecta a **telnetd de GNU Inetutils**, que es el servicio encargado de permitir conexiones remotas a un sistema mediante el protocolo Telnet.

GNU Inetutils es un paquete de software del proyecto GNU Project que proporciona implementaciones libres de utilidades básicas de red. Incluye programas cliente y servidor que reemplazan a los equivalentes tradicionales de Unix, con el objetivo de ofrecer alternativas mantenidas y compatibles con los estándares.

La vulnerabilidad se origina por un desbordamiento de búfer durante la fase inicial de conexión (antes de la autenticación), cuando el servicio procesa solicitudes manipuladas. Un atacante remoto no autenticado puede explotar esta falla simplemente conectándose al **puerto 23**, sin necesidad de credenciales ni interacción del usuario.

A nivel global, se estima que existen aproximadamente **1,300,000 dispositivos potencialmente afectados**, ya que mantienen el **puerto 23 (Telnet) expuesto a Internet**. Estos sistemas representan un objetivo atractivo para los atacantes, quienes podrían intentar explotarlos para obtener acceso no autorizado o comprometer la infraestructura.



Si el servicio telnetd se ejecuta con privilegios elevados (como root), una explotación exitosa puede permitir el control total del sistema, incluyendo:

- Ejecución remota de código
- Instalación de puertas traseras
- Exfiltración de información sensible

Solución y mitigaciones:

- Actualizar a la versión corregida de GNU Inetutils en cuanto esté disponible
- Deshabilitar el servicio Telnet si no es estrictamente necesario.
- Bloquear el puerto 23 en firewalls perimetrales.

Información adicional:

- https://thehackernews.com/2026/03/critical-telnetd-flaw-cve-2026-32746.html
- https://securityaffairs.com/189620/hacking/researchers-warn-of-unpatched-critical-telnetd-flaw-affecting-all-versions.html

https://www.tenable.com/cve/CVE-2026-32746