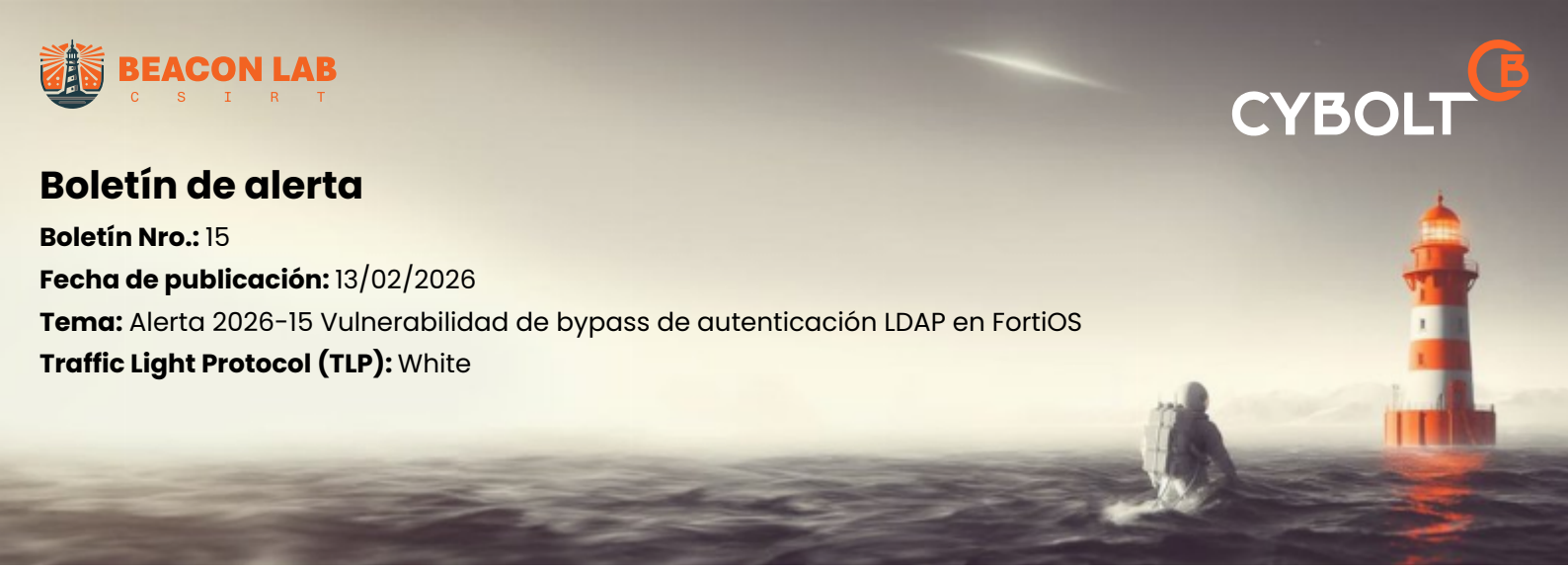


Boletín de alerta

Boletín Nro.: 15
Fecha de publicación: 13/02/2026
Tema: Alerta 2026-15 Vulnerabilidad de bypass de autenticación LDAP en FortiOS
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **FortiOS versiones 7.6.0 hasta 7.6.4** cuando se configura para usar autenticación LDAP con servidores que permiten enlaces anónimos o no estrictos.

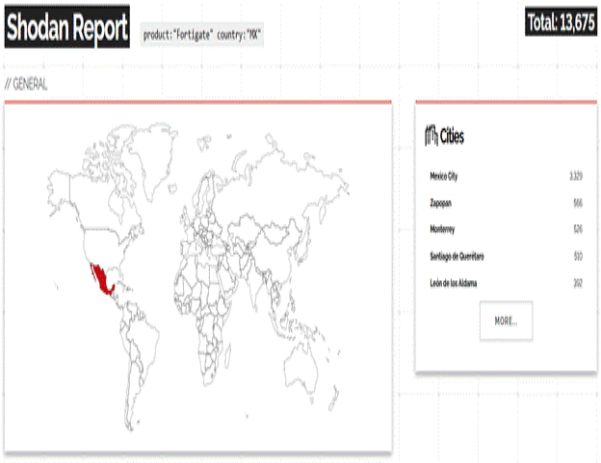
Descripción

Recientemente se identificó la vulnerabilidad CVE-2026-22153, clasificada como *Authentication Bypass by Primary Weakness* (CWE-305), que afecta a dispositivos FortiOS que utilizan políticas de acceso basadas en LDAP para funcionalidades como Agentless VPN o Fortinet Single Sign-On (FSSO).

FortiOS verifica credenciales LDAP como parte del proceso de autenticación de usuarios remotos. Debido a una implementación permisiva al interactuar con servidores LDAP configurados para aceptar enlaces sin autenticación, un atacante no autenticado puede eludir por completo la verificación LDAP, obteniendo acceso a funciones restringidas sin necesidad de credenciales válidas.

Si bien esta falla no permite ejecución arbitraria de código en el dispositivo directamente, sí importa en el contexto de control de acceso: un atacante puede conseguir acceso no autorizado a políticas de red protegidas (por ejemplo, acceso a VPN sin login), lo que puede derivar en acceso a recursos internos corporativos y pérdida de confidencialidad e integridad.

Según datos de Shodan.io, en México hay más de 13 mil dispositivos Fortigate implementados, que si bien no todos pueden llegar a ser vulnerables, al menos los que están en el rango de versiones afectadas lo son, por lo que es necesario verificar la versión y actualizar en caso de ser necesario.



Dispositivos Fortigate en México

Mitigaciones y soluciones

Parche y actualización

- Fortinet ha publicado actualizaciones que abordan esta vulnerabilidad. Se recomienda actualizar a FortiOS 7.6.5 o posteriores donde se corrige el bypass de autenticación, mismos que puedes descargar en el siguiente link: https://www.fortiguard.com/psirt/FG-IR-25-1052

Configuración segura

- Revisar y restringir los parámetros de autenticación LDAP para evitar configuraciones que permitan enlaces anónimos o no seguros.
- Asegurar que los servidores LDAP backend no acepten *anonymous binds*.
- Limitar el acceso a interfaces de administración y gestión del firewall, idealmente detrás de redes de gestión segregadas.

Hardening adicional

- Implementar monitorización y alertas sobre intentos fallidos/inusuales de acceso LDAP o intentos de bypass.
- Aplicar seguridad en capas (por ejemplo MFA) para puntos de entrada como VPN, reduciendo la dependencia exclusiva de LDAP para autenticación.

Información adicional:

- **https://www.tenable.com/plugins/nessus/298512**
- **Blog elhacker.NET: Vulnerabilidad en FortiOS permite a atacantes eludir autenticación LDAP**
- **CVE-2026-22153 : An Authentication Bypass by Primary Weakness vulnerability [CWE-305] vulnerabili**