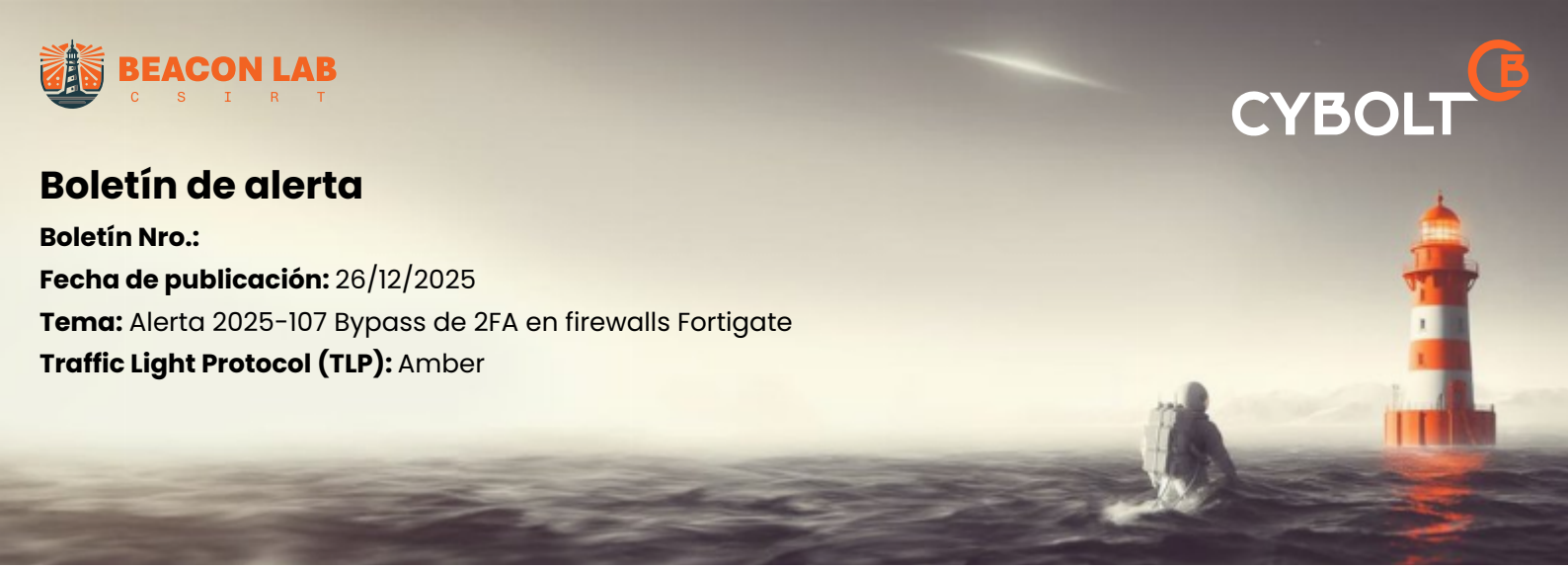


Boletín de alerta

Boletín Nro.:
Fecha de publicación: 26/12/2025
Tema: Alerta 2025-107 Bypass de 2FA en firewalls Fortigate
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Fortinet FortiGate (Firewalls) — versiones antiguas sin parches que no incluyen la corrección de CVE-2020-12812, específicamente en configuraciones donde:

- Usuarios locales con 2FA están asociados a grupos LDAP, donde esos grupos se usan en políticas de autenticación (VPN o acceso administrativo).

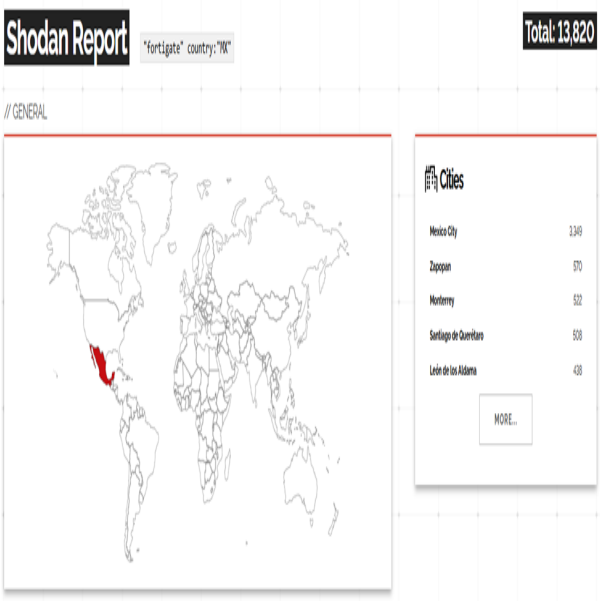
Descripción

Recientemente se ha observado explotación activa de una vulnerabilidad vieja en dispositivos FortiGate de Fortinet que permite **omitir la autenticación de dos factores (2FA)** en VPNs y consolas administrativas. Esta falla, identificada como **CVE-2020-12812**, fue originalmente parcheada en **2020**, pero aún permanece explotable en entornos desactualizados o mal configurados.

La raíz del problema se encuentra en la **manera en la que FortiGate compara nombres de usuario frente a servidores LDAP**. Mientras que muchos LDAP como Active Directory no distinguen entre mayúsculas y minúsculas, FortiGate aplica sensibilidad a caso por defecto. Un atacante puede entonces enviar variantes de un nombre de usuario (p.ej. “DSanchez” en lugar de “dsanchez”), provocando que FortiGate no coincida con el usuario local y recurra a una política secundaria basada en LDAP para autenticar al usuario con credenciales LDAP válidas. Este proceso evita por completo el paso de 2FA, **concediendo acceso sin token a interfaces VPN o de administración**.

Debido a esta lógica, si un usuario local con 2FA está en un grupo LDAP que se usa en la política de acceso, el atacante puede entrar al sistema simplemente con que las credenciales LDAP permitan el inicio de sesión, **sin necesidad de pasar la segunda capa de autenticación.**

Según datos de Shodan.io**, en México se identifican más de 13 mil firewalls de Fortigate**, por lo que se recomienda encarecidamente tomar acciones y en caso de ser necesario, actualizar los firewalls.



Número de firewalls de Fortigate implementados en México

Mitigaciones y soluciones

Para reducir el riesgo y eliminar esta vía de explotación:

1. **Actualizar firmware de FortiGate** a versiones que incluyan la corrección de **CVE-2020-12812**, como se indica en las versiones posteriores a 6.0.10, 6.2.4 y 6.4.1 o superiores en el siguiente enlace:

https://www.fortiguard.com/psirt/FG-IR-19-283

2. En dispositivos que aún no puedan actualizarse, **deshabilitar la sensibilidad a mayúsculas/minúsculas** para los nombres de usuario en FortiOS. Esto evita que el bypass funcione.
3. **Revisar y ajustar las configuraciones LDAP/SSO** eliminando mapeos de grupos innecesarios en políticas de autenticación (especialmente para usuarios con 2FA).
4. **Auditar logs de autenticación** para detectar patrones de intentos con variaciones de nombre de usuario (indicadores típicos de este tipo de bypass).
5. Considerar **limitaciones de gestión de acceso** (p.ej., administración segura desde redes internas, listas blancas de IPs para administración) para reducir la exposición directa de interfaces críticas a Internet.

Información adicional:

- https://www.fortinet.com/blog/psirt-blogs/product-security-advisory-and-analysis-observed-abuse-of-fg-ir-19-283
- https://cybersecuritynews.com/fortigate-firewall-vulnerability/
- https://nvd.nist.gov/vuln/detail/CVE-2020-12812