BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-62
Fecha de publicación: 05/11/2024
Tema: Vulnerabilidad crítica de XSS en pfSense
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- pfSense versión 2.5.2

Descripción

Recientemente se ha detectado una explotación activa de la vulnerabilidad identificada como **CVE-2024-46538** en **pfSense versión 2.5.2** de criticadad critica y con un score de **CVSSv3 de 9.3.** Esta vulnerabilidad, de tipo Cross Site Script almacenado (Stored XSS) permite a atacantes ejecutar scripts web o código HTML arbitrario mediante la inyección de una carga maliciosa en la variable $pconfig en el archivo interfaces_groups_edit.php.

PfSense es un sistema operativo de código abierto basado en FreeBSD que funciona como firewall y router, siendo una de las soluciones más populares en el ámbito de la seguridad de redes. Ofrece características avanzadas como firewall stateful, VPN (OpenVPN e IPsec), sistema de prevención de intrusiones, balanceo de carga, portal cautivo, y capacidades de VLAN y QoS. Su interfaz web intuitiva, junto con su naturaleza gratuita y altamente configurable, lo hace especialmente atractivo para pequeñas y medianas empresas, instituciones educativas y profesionales de TI que buscan una solución robusta de seguridad sin costos de licenciamiento.

Es importante destacar que la explotación de esta vulnerabilidad, **CVE-2024-46538**, requiere que el atacante tenga acceso al sistema pfSense y la capacidad de inyectar cargas maliciosas en la interfaz web, lo que implica que el atacante debe tener privilegios de usuario autenticado en el sistema.

Ya se encuentran disponible PoC que afectan dicha vulnerabilidad, la existencia de un PoC (Proof of Concept) disponible para un CVE implica un riesgo significativamente elevado, ya que transforma una vulnerabilidad teórica en una amenaza práctica y explotable, recomendamos tomar medidas de mitigación la mas pronto posible.

Según datos de Netlas, se han identificado casi **800 dispositivos pfSense expuestos en México**. Dado que la vulnerabilidad **CVE-2024-46538** afecta a pfSense versión 2.5.2, es crucial que los administradores de estos dispositivos verifiquen sus versiones y apliquen las actualizaciones de seguridad correspondientes para mitigar posibles riesgos.

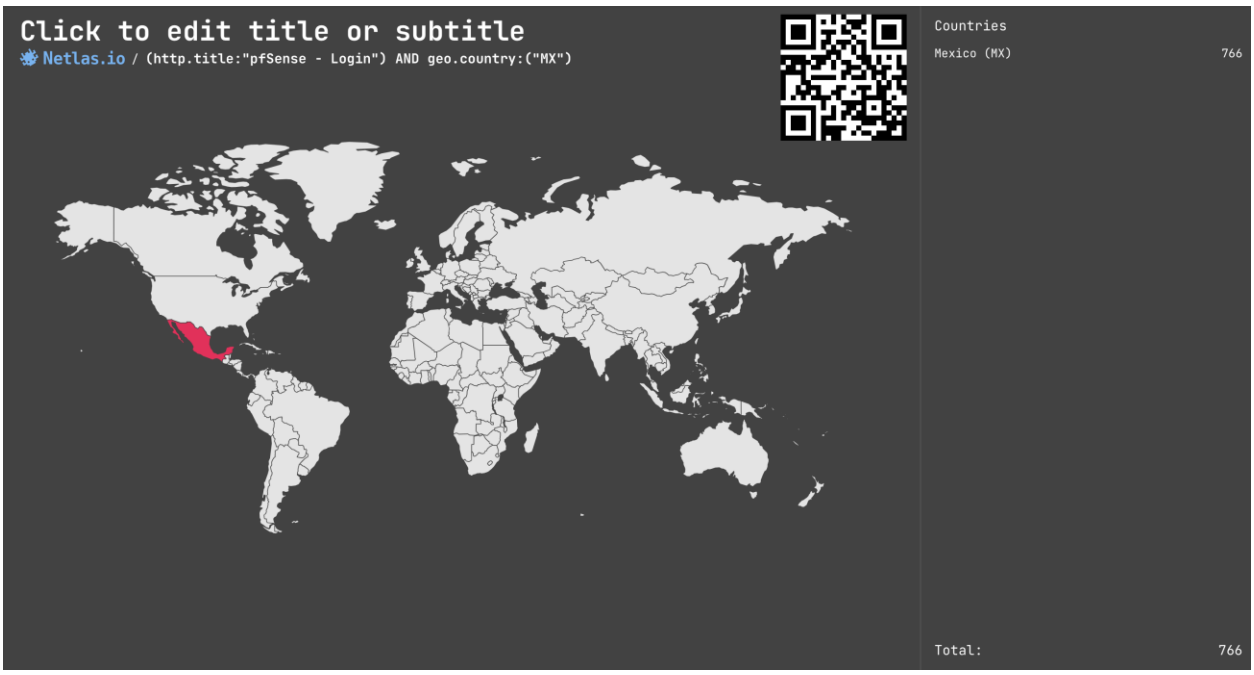

Figura 1 Captura de pantalla del sitio Netlas.io https://nt.ls/6w9g3

Solución

Se recomienda actualizar pfSense a la versión más reciente que contenga las correcciones de seguridad pertinentes para mitigar este riesgo, puede realizarlo directaente desde del panel de administración web del pfsense o pueden obtener las ultimas version en el siguiente enlace: https://www.pfsense.org/download/

Para mas información sobre la vulnerabilidad puede consultar el siguiente ticket creado por el equipo de pfSense: https://redmine.pfsense.org/issues/15778

Información adicional:

- Netlas | Responses | Dispositivos pfSense en Mexico
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-46538
- https://securityonline.info/cve-2024-46538-unpatched-xss-flaw-in-pfsense-allows-remote-exploits-poc-published/
- https://redmine.pfsense.org/issues/15778

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com