BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-03
Fecha de publicación: 09/02/2024
Tema: Fortinet advierte que una vulnerabilidad en FortiOS SSL VPN está siendo explotada.
Traffic Light Protocol (TLP): White

Producto afectado:

- FortiOS-SSL-VPN:

FortiOS 7.4: 7.4.0 a la 7.4.2
FortiOS 7.2: 7.2.0 a la 7.2.6
FortiOS 7.0: 7.0.0 a la 7.0.13
FortiOS 6.4: 6.4.0 a la 6.4.14
FortiOS 6.2: 6.2.0 a la 6.2.15
FortiOS 6.0: Todas las versiones 6.0

- Descripción:

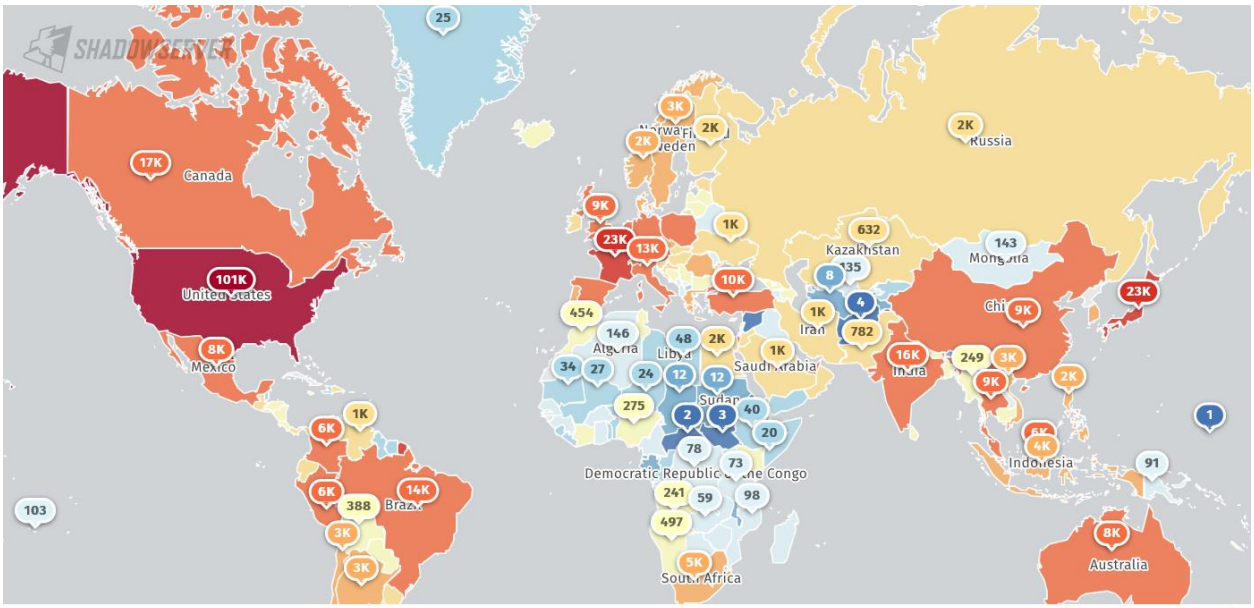
Fortinet está advirtiendo que una nueva vulnerabilidad crítica de ejecución de código remoto en **FortiOS SSL VPN** está siendo potencialmente explotada

Aunque, CISA (Cybersecurity & Infrastructure Security Agercy) **afirma que actualmente ya se encontraron explotaciones** de la vulnerabilidad del producto.

La vulnerabilidad conocida como **CVE-2024-21762** / FG-IR-24-015 cuenta con una puntuación de severidad de 9.6, esta, permite una escritura “out-opf-bounds” (El producto escribe datos más allá del final o antes del comienzo del búfer previsto.), lo que permite a los atacantes remotos no autenticados la ejecución arbitraria de código o comandos a través de peticiones malintencionadas de HTTP.

Debido a la alta severidad de la nueva vulnerabilidad CVE-2024-21762 y la alta probabilidad de que pueda ser explotada, se recomienda encarecidamente **realizar el parcheo o el “workaround” inmediatamente.**

De acuerdo con los datos de la plataforma ShadowServer, en México, existen alrededor de **8,000** dispositivos FortiOS SSL-VPN **expuestos a internet** y **en E.U.A**, más de **100,000**.



Impacto

La explotación de esta vulnerabilidad permite la ejecución arbitraria de código o comandos, que posteriormente puede aseverar el impacto del ataque. Por ejemplo, utilizar de pivote el dispositivo FortiOS para infectar la red interna o realizar movimientos laterales,

Solución

El fabricante (Fortinet), explica que las vulnerabilidades pueden ser corregidas al instalar las siguientes versiones en sus productos:

- Versiones que solucionan la vulnerabilidad CVE-2024-21762:

FortiOS 7.4: Actualizar a 7.2.7 o mayor.
FortiOS 7.2: Actualizar a 7.0.14 o mayor
FortiOS 7.0: Actualizar a 6.4.15 o mayor
FortiOS 6.4: Actualizar a 6.2.16 o mayor
FortiOS 6.2: Actualizar a 7.4.3 o mayor
FortiOS 6.0: Migrar a una versión con arreglo

El equipo **Beacon Lab** también aconseja con insistencia, realizar la actualización a estas versiones lo más pronto posible.

Mitigación

El fabricante (Fortinet), recomienda el “workaround” de deshabilitar el SSL-VPN de los dispositivos FortiOS si es que no podemos aplicar el parche a nuestros dispositivos FortiOS.

Información adicional:

- https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/amp/
- https://www.fortiguard.com/psirt/FG-IR-24-015
- https://cyber.vumetric.com/security-news/2024/02/08/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/
- https://dashboard.shadowserver.org/statistics/iot-devices/map/?day=2024-02-08&vendor=fortinet&type=vpn&model=fortios+ssl-vpn&tag=all&geo=all&data_set=count&scale=log
- https://cwe.mitre.org/data/definitions/787.html
- https://nvd.nist.gov/vuln/detail/CVE-2024-21762
- CISA Adds One Known Exploited Vulnerability to Catalog | CISA

BEACON LAB
C S I R T

info@beaconlab.mx

beaconlab.mx

CYBOLT
Security Innovation

contact@cybolt.com

cybolt.com