GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

ACTUALIZACIÓN FIRMWARE FIREWALL 601E

MINISTERIO DE AGRICULTURA.

Caso No: 00056126

Descripción breve

Actualizar el FortGate de la versión 7.0.9 a la versión 7.0.12 por la vulnerabilidad CVE-2023-27997

Ing. Juan Jose Carvajal
juan.carvajal@gammaingenieros.com

TABLA DE CONTENIDO

1. Resumen:

Debido a la vulnerabilidad CVE-2023-27997, se ha llevado a cabo un proceso de actualización en los equipos Firewall Fortinet. Esta vulnerabilidad afecta principalmente a las SSL-VPN, ya que puede permitir que un atacante remoto ejecute código o comandos mediante solicitudes diseñadas específicamente.

La vulnerabilidad afecta principalmente a las siguientes versiones de FortiOS:

FortiOS versión 7.2.0 a 7.2.4

FortiOS versión 7.0.0 a 7.0.11

FortiOS versión 6.4.0 a 6.4.12

FortiOS versión 6.0.0 a 6.0.16

En nuestro caso, el Firewall Fortinet se encontraba en la versión 7.0.9, lo que implicaba un riesgo de seguridad. Por tanto, se ha procedido a realizar la actualización a la versión 7.0.12, la cual mitiga y soluciona esta vulnerabilidad. Esta medida es fundamental para garantizar la integridad y seguridad de nuestros sistemas.

2. Actividades Realizadas:

Primero, se realiza una exhaustiva revisión del funcionamiento del Firewall en la versión 7.0.9, donde se valida el correcto funcionamiento de sus diferentes configuraciones, en especial aspectos como políticas, estado del equipo y sistema. Es importante mencionar que el Firewall está configurado en modo de alta disponibilidad (HA) y cuenta con un equipo de respaldo.

Durante esta revisión, se recolectan las evidencias necesarias mediante capturas de pantalla, con el objetivo de documentar el estado actual del Firewall antes de proceder con la actualización.

Una vez completada la revisión y tomadas las evidencias, se da inicio al proceso de actualización del Firewall Fortinet a la versión 7.0.12. Este proceso se realiza siguiendo las mejores prácticas recomendadas por el fabricante y asegurando la disponibilidad de los servicios críticos.

Durante la actualización, se llevan a cabo las pruebas necesarias para verificar el correcto funcionamiento del Firewall en la nueva versión y se realizan las configuraciones adicionales pertinentes para garantizar una transición sin problemas.

Es importante mencionar que se sigue un enfoque cuidadoso y metodológico durante todo el proceso de actualización, con el objetivo de minimizar cualquier impacto en la operación y asegurar la continuidad del servicio.

Una vez finalizada la actualización, se realizan las pruebas de funcionalidad y seguridad correspondientes para confirmar que el Firewall está operando de manera óptima en la versión 7.0.12.

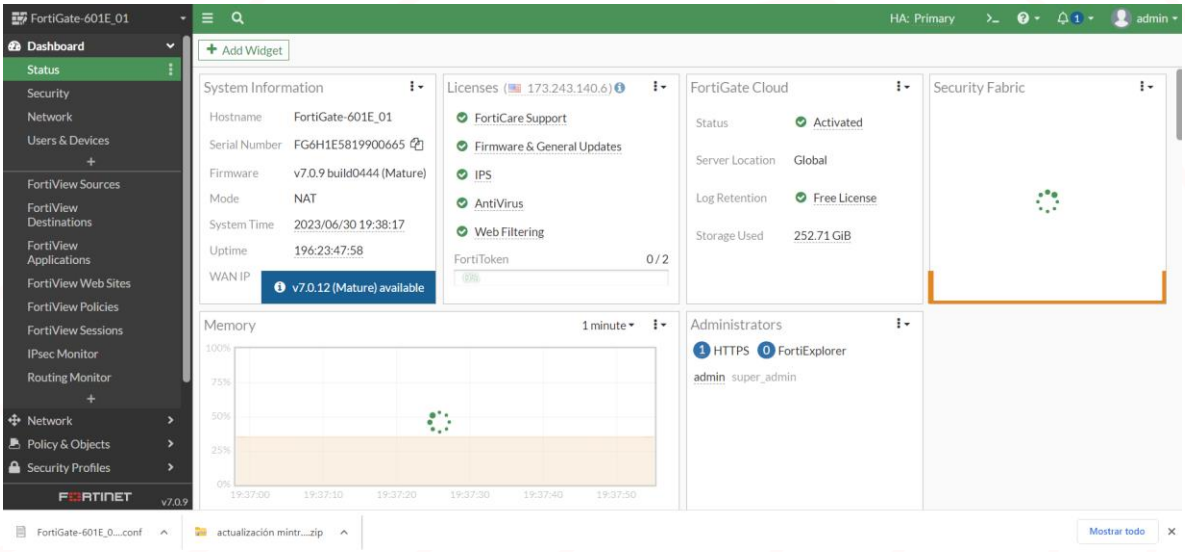

Imagen 1

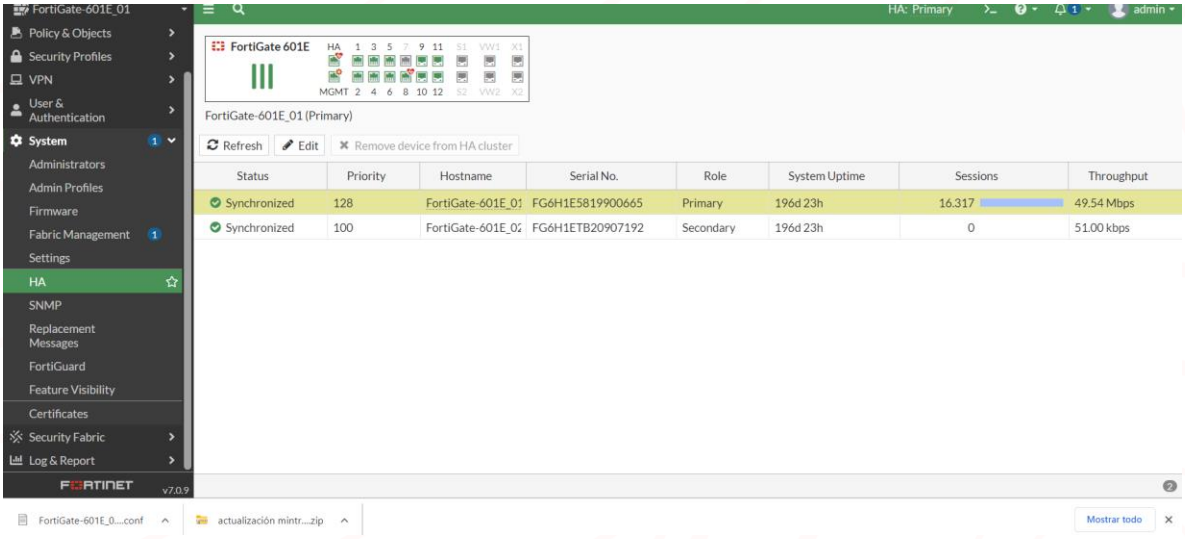

Imagen 2

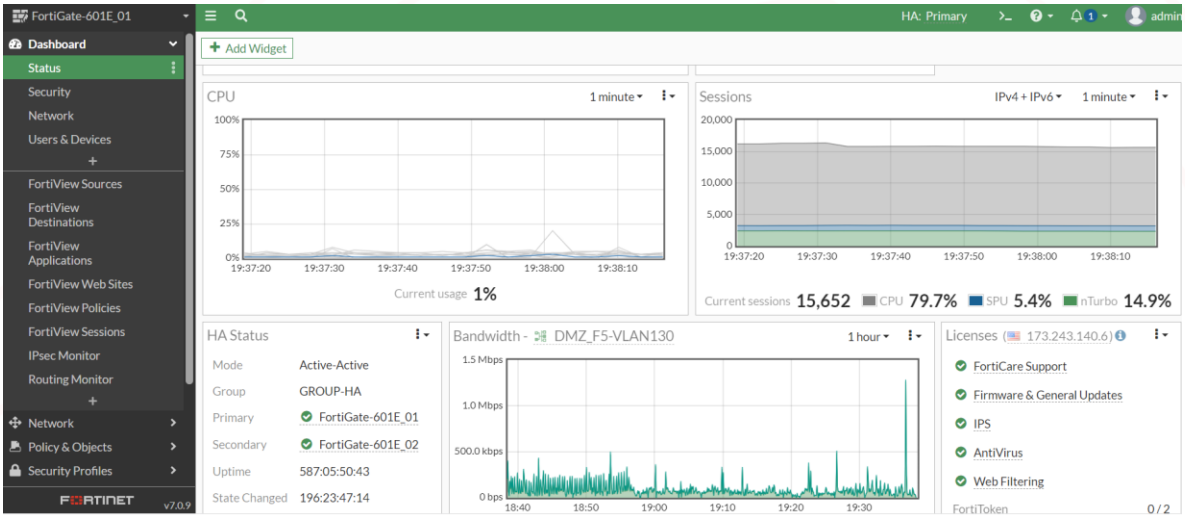
FortiGate-601E_01
HA: Primary
admin
Dashboard
Status
Security
Network
Users & Devices
FortiView Sources
FortiView Destinations
FortiView Applications
FortiView Web Sites
FortiView Policies
FortiView Sessions
IPsec Monitor
Routing Monitor
Network
Policy & Objects
Security Profiles
FORTINET
v7.0.9
Add Widget
CPU
1 minute
100%
75%
50%
25%
0%
19:37:20
19:37:30
19:37:40
19:37:50
19:38:00
19:38:10
Current usage 1%
Sessions
IPv4 + IPv6
1 minute
20,000
15,000
10,000
5,000
0
Current sessions 15,652
CPU 79.7%
SPU 5.4%
nTurbo 14.9%
HA Status
Mode Active-Active
Group GROUP-HA
Primary FortiGate-601E_01
Secondary FortiGate-601E_02
Uptime 587:05:50:43
State Changed 196:23:47:14
Bandwidth - DMZ_F5-VLAN130
1 hour
1.5 Mbps
1.0 Mbps
500.0 kbps
0 bps
18:40
18:50
19:00
19:10
19:20
19:30
Licenses (173.243.140.6)
FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken
0 / 2

Imagen 3

A continuación, se comparten las imágenes donde se observa la actualización final 7.0.12

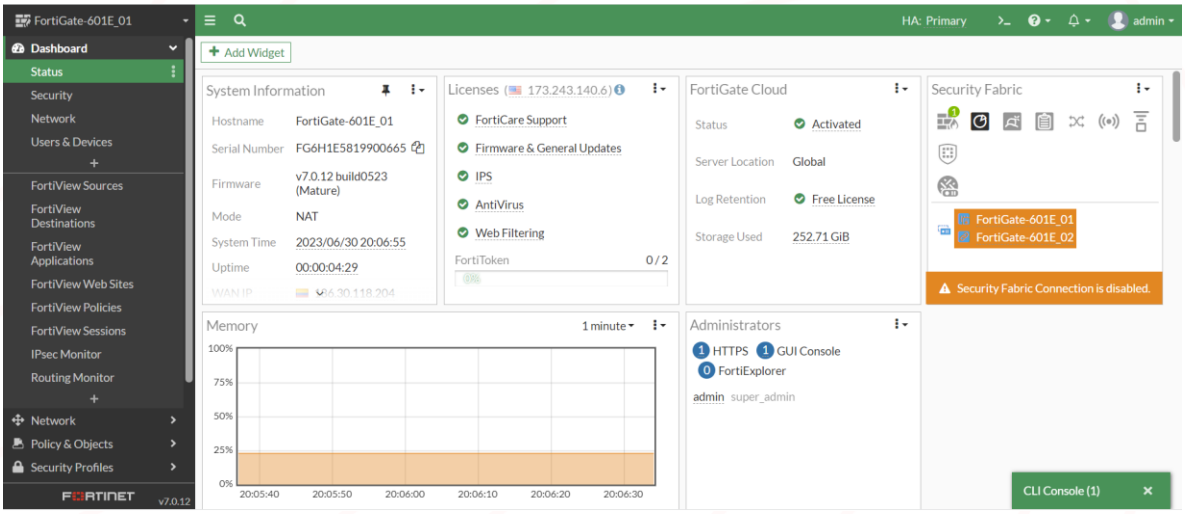

Imagen 8

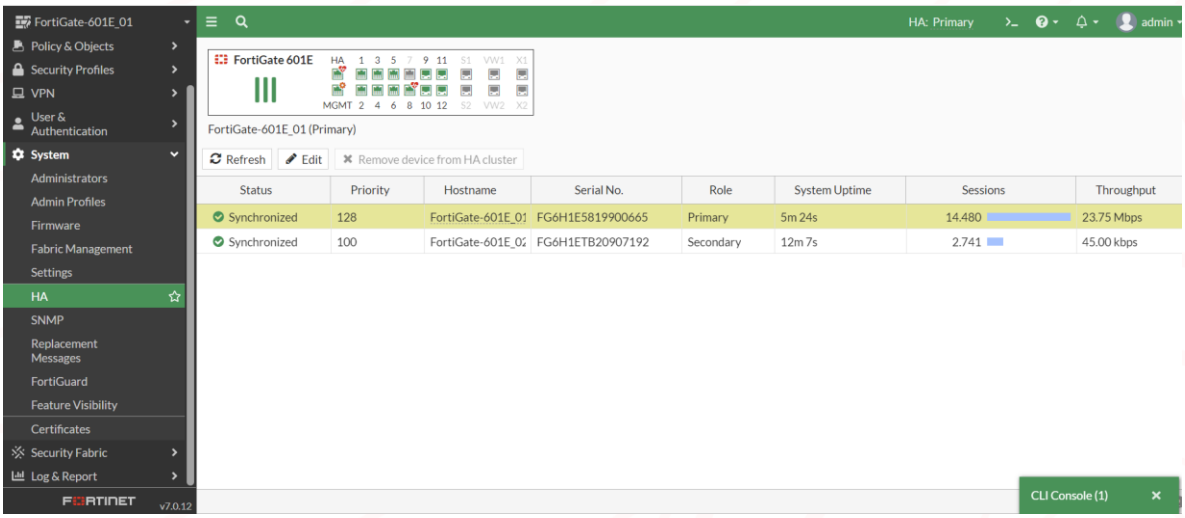

Imagen 9

Se valida la correcta sincronización con FortiAnalizer

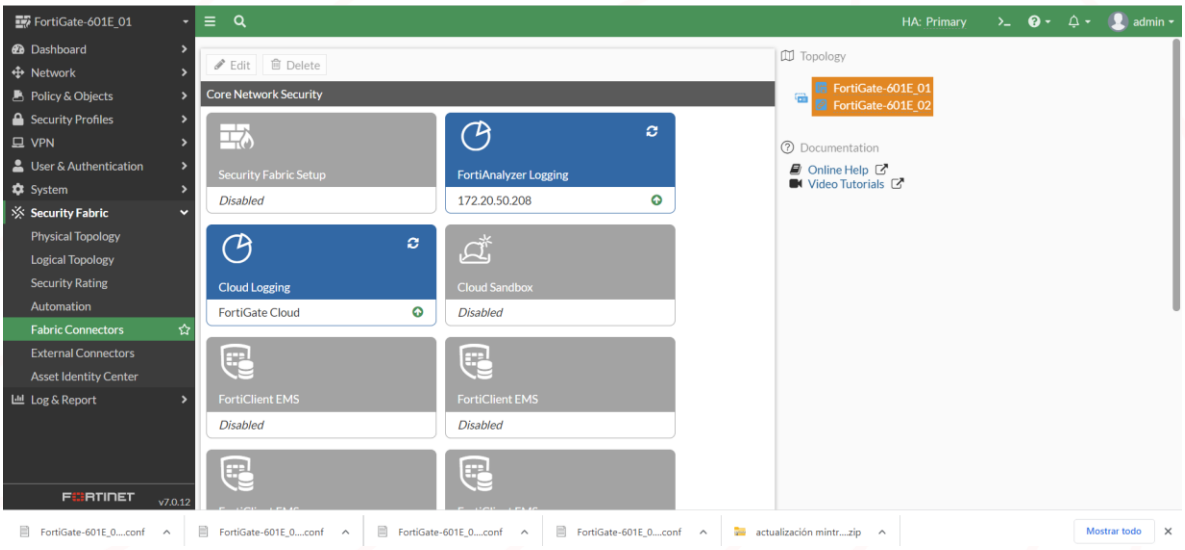

Imagen 10

3. Conclusiones:

- El proceso de actualización resultó exitoso, permitiendo así solucionar la vulnerabilidad CVE-2023-27997 y actualizar los equipos Firewall Fortinet a la versión 7.0.12 de manera satisfactoria.

- Durante la actualización, se pudo constatar un funcionamiento adecuado de los equipos firewall Fortinet, lo cual es un indicativo positivo de la efectividad y estabilidad de la actualización realizada.

- En resumen, el proceso de actualización se llevó a cabo de manera planificada, cuidadosa y documentada, garantizando así un correcto funcionamiento del Firewall en la nueva versión y la continuidad de los servicios críticos.