BOLETÍN DE ALERTA

Boletín Nro.: 2023-07
Fecha de publicación: 13/03/2023
Tema: Vulnerabilidad crítica de desbordamiento de *buffer* (*BoF*) en Fortinet

Software afectado:

- FortiOS, versiones:
  - 7.2.0 hasta 7.2.3,
  - 7.0.0 hasta 7.0.9,
  - 6.4.0 hasta 6.4.11,
  - 6.2.0 hasta 6.2.12,
  - 6.0 (todas las versiones).
- FortiProxy, versiones:
  - 7.2.0 hasta 7.2.2,
  - 7.0.0 hasta 7.0.8,
  - 2.0.0 hasta 2.0.11,
  - 1.2 y 1.1 (todas las versiones).

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad crítica que afecta a productos Fortinet, que permitiría a un atacante realizar desbordamiento de *buffer* en el sistema afectado.

La vulnerabilidad identificada como CVE-2023-25610, de severidad “Crítica” y con puntuación de 9.3. Esta vulnerabilidad de desbordamiento de *buffer* se debe a una falla de seguridad en la interfaz administrativa de FortiOS y FortiProxy. Esto permitiría a un atacante remoto no autenticado a través del envío de solicitudes específicamente diseñadas, realizar ejecución arbitraria de código y provocar denegación de servicios (*DoS*) en el sistema afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ejecución arbitraria de código y provocar denegación de servicios (*DoS*) en el sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/596131

Mitigación:

Adicionalmente, como mitigación temporal recomendamos deshabilitar y/o limitar la interfaz administrativa por HTTP y/o HTTPS para ello puede seguir los siguientes pasos:

1. Limitar las direcciones *IP* accesibles.

```
config firewall address
edit "my_allowed_addresses"
set subnet <MY IP> <MY SUBNET>
end
```

2. Luego crear grupo de direcciones:

```
config firewall addrgrp
edit "MGMT_IPs"
set member "my_allowed_addresses"

end
```

3. Crear una Política Local (**Local in Policy**) para restringir el acceso solo al grupo predeterminado a la interfaz de administración (puerto 1):

```
config firewall local-in-policy
edit 1
set intf port1
set srcaddr "MGMT_IPs"
set dstaddr "all"
set action accept
set service HTTPS HTTP
set schedule "always"
set status enable
next
edit 2
set intf "any"
set srcaddr "all"
set dstaddr "all"
set action deny
set service HTTPS HTTP
set schedule "always"
set status enable
end
```

4. En caso de no utilizar los puestos predeterminados, crear el objeto de servicio correspondiente para el acceso administrativo del GUI:

```
config firewall service custom
edit GUI_HTTPS
set tcp-portrange <admin-sport>
next
edit GUI_HTTP
```

```
set tcp-portrange <admin-port>

end
```

5. Finalmente, utilizar estos objetos en lugar de "HTTP HTTPS" en **Local in Policy** 1 y 2.

Nota: Cuando es utilizada una interfaz administrativa de alta disponibilidad la Política Local (**Local in Policy)** debe ser configurada de manera diferente, para más información acceder al siguiente enlace.

Información adicional:

- https://www.helpnetsecurity.com/2023/03/09/cve-2023-25610/
- https://www.fortiguard.com/psirt/FG-IR-23-001
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610
- https://www.fortiguard.com/psirt/cvrf/FG-IR-23-001
- https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-local-in-policy-on-a-HA/ta-p/222005
- https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/596131