BOLETÍN DE ALERTA

Boletín Nro.: 2022-41
Fecha de publicación: 11/10/2022
Tema: Vulnerabilidad de omisión de autenticación en FortiGate y FortiProxy

Las versiones afectadas son:

- FortiOS, versión 7.0.0 a 7.0.6.
- FortiOS, versión 7.2.0 a 7.2.1.
- FortiProxy, versión 7.0.0 a 7.0.6 y 7.2.0.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a FortiGate y FortiProxy, que permitiría a un atacante no autenticado realizar operaciones arbitrarias en la interfaz administrativa.

La vulnerabilidad identificada como CVE-2022-40684, de severidad "crítica", con una puntuación asignada de 9.6. Esta vulnerabilidad se debe a una falla en el componente *Administrative Interface.* Esto permitiría a un atacante no autenticado realizar operaciones arbitrarias en la interfaz administrativa. Actualmente para esta vulnerabilidad existe un *PoC* que si bien no se publicó todavía, se publicará en los próximos días.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado realizar operaciones arbitrarias en la interfaz administrativa.

Solución:
Se recomienda acceder a las actualizaciones correspondientes provistas por el proveedor en el siguiente enlace:

- https://support.fortinet.com/welcome/#/

En caso de no haber aplicado los parches correspondientes, es recomendable seguir los siguientes pasos de mitigación:

FortiOS:

1. Deshabilitar la interfaz administrativa *HTTP*/*HTTPS* o Limitar las direcciones IP que pueden llegar a la interfaz administrativa:

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

2. Crear un grupo de direcciones:

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

3. Configurar el firewall local para poder restringir el acceso al grupo predefinido en la interfaz de administración:

```
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 "all"
set srcaddr "all"
set dstaddr "all"
set action deny
set service HTTPS HTTP
set schedule "always"
set status enable
end
```

4. Si se está utilizando puertos no predeterminados, se debe crear el objeto de servicios adecuado para el acceso administrativo de la GUI:

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

```
edit GUI_HTTP
set tcp-portrange <admin-port>
end
```

FortiProxy:

Deshabilitar la interfaz administrativa *HTTP*/*HTTPS* o Limitar las direcciones IP que pueden llegar a la interfaz administrativa:

```
config system interface
edit port1
set dedicated-to management
set trust-ip-1 <MY IP> <MY SUBNET>
end
```

Adicionalmente, se recomienda a los usuarios desactivar el acceso administrativo a la interfaz externa (orientada a Internet), hasta que se puedan implementar las actualizaciones o aplicar una política de firewall que defina solo "*tráfico de entrada local*".

Información adicional:

- https://thehackernews.com/2022/10/fortinet-warns-of-new-auth-bypass-flaw.html
- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1381/
- https://www.bleepingcomputer.com/news/security/fortinet-warns-admins-to-patch-critical-auth-bypass-bug-immediately/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40684
- https://support.fortinet.com/welcome/#/