BOLETÍN DE ALERTA

Boletín Nro.: 2023-33
Fecha de publicación: 18/07/2023
Tema: Vulnerabilidad crítica de *RCE* en FortiOS y FortiProxy

Software afectado:

- FortiOS versión 7.2.0 a 7.2.3.
- FortiOS versión 7.0.0 a 7.0.10.
- FortiProxy versión 7.2.0 a 7.2.2.
- FortiProxy versión 7.0.0 a 7.0.9.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a FortiOS y FortiProxy de Fortinet, que permitiría a un atacante realizar ejecución remota de código (*RCE*).

La vulnerabilidad identificada como CVE-2023-33308 de severidad "Crítica", con puntuación de 9.8. Esta vulnerabilidad del tipo *Stack-Based Buffer Overflow* se debe a una falla en la función encargada de inspeccionar las políticas de *proxy* o políticas de *firewall* con modo proxy e inspección profunda de paquetes *SSL* habilitados en FortiOS y FortiProxy. Esto permitiría a un atacante remoto a través del envío de paquetes especialmente diseñados, realizar ejecución remota de código (*RCE*) o ejecución arbitraria de comandos en el dispositivo afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto realizar ejecución remota de código (*RCE*) o ejecución arbitraria de comandos en el dispositivo afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en el siguiente enlace:

- https://www.fortiguard.com/psirt/FG-IR-23-183

Adicionalmente, como medida adicional de mitigación se recomienda deshabilitar la compatibilidad con *HTTP/2* en los perfiles de inspección *SSL* utilizados por las directivas de *proxy* o las directivas de *firewall* con modo *proxy*, un ejemplo de este sería:

```
config firewall ssl-ssh-profile

   edit «custom-deep-inspection»

      set supported-alpn http1-1

   next

end
```

Información adicional:

- https://blog.elhacker.net/2023/07/la-cuarta-grave-vulnerabilidad-en-fortinet-fortios.html
- https://www.cert.gov.py/noticias/vulnerabilidad-de-stack-based-buffer-overflow-y-autenticacion-inapropiada-en-productos-fortinet/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33308
- https://www.fortiguard.com/psirt/FG-IR-23-183