BOLETÍN DE ALERTA

Boletín Nro.: 2021-38

Fecha de publicación: 14/12/2021

Tema: Múltiples vulnerabilidades detectadas en Fortinet

Dispositivos afectados:

- **CVE-2021-26103**
  - FortiProxy versiones anteriores a 2.0.4
  - FortiProxy versiones anteriores a 1.2.12
  - FortiGate las versiones anteriores a 7.0.1
  - FortiGate las versiones anteriores a 6.4.7

- **CVE-2021-26109**
  - FortiOS versiones anteriores a 7.0.1.
  - FortiOS versiones anteriores a 6.4.6.

- **CVE-2021-26110**
  - FortiOS versiones anteriores a 7.0.1.
  - FortiOS versiones anteriores a 6.4.7.
  - Modelos F-Series (FG-1800F, FG-3800F, FG-4200F, FG-4400F) versiones anteriores a 6.2.9.
  - FortiProxy versiones anteriores a 2.0.2.
  - FortiProxy versiones anteriores a 1.2.10.

Descripción:

Se han identificado un total de tres fallos de seguridad que afectan a diferentes versiones del software de Fortinet, éstos pueden ser explotados por un usuario malintencionado para escalar privilegios, causar denegación de servicio y/o ejecutar comandos remotamente en el software vulnerable.

A continuación, se describen las vulnerabilidades:

CVE-2021-26103 de severidad alta con una puntuación de 8.8, se debe a una falla en la verificación de la autenticidad de los datos en la interfaz de usuario lo que permitiría a un atacante no autenticado llevar a cabo un ataque de Cross-Site Request Forgery (CSRF).

CVE-2021-26109 de severidad crítica con una puntuación de 9.8, se debe a una vulnerabilidad de *integer overflow* en el SSLVPN de FortiOS, esto permitiría a un atacante no autenticado la ejecución de código a través de la creación de peticiones SSLVPN maliciosas.

CVE-2021-26110 de severidad alta con una puntuación de 7.8, se debe a una falla en el control de acceso en FortiOS y en FortiProxy que permitiría al atacante que se encuentra autenticado con bajos privilegios realizar un escalamiento de privilegios tomando el control del usuario *super_admin* por medio de la creación de un script de configuración malicioso.

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante ejecutar código malicioso en el sistema y obtener el control total del sistema afectado.

Solución:

Se recomienda actualizar a la versión más reciente del software instalado en el dispositivo afectado:

- https://www.fortinet.com/support/product-downloads

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2021-26109
- https://nvd.nist.gov/vuln/detail/CVE-2021-26103
- https://nvd.nist.gov/vuln/detail/CVE-2021-26110
- https://www.fortiguard.com/psirt/FG-IR-20-158