BOLETÍN DE ALERTA

Boletín Nro.: 2021-16

Fecha de publicación: 21/07/2021

Tema: Vulnerabilidad en los productos FortiManager y FortiAnalyzer de Fortinet.

Productos afectados:

- FortiAnalyzer y FortiManager:
    - Versiones 5.6.11 y anteriores.
    - Versiones 6.0.10 y anteriores
    - Versiones 6.2.7 y anteriores
    - Versiones 6.4. y anteriores
    - Versión 7.0.0

- FortiManager versiones 5.4.x.

Descripción:

Fortinet ha informado la existencia de una vulnerabilidad UAF (Use-After-Free) en el demonio fgfmsd de FortiManager y FortiAnalyzer, identificada como CVE-2021-32589, con una puntuación CVSSv3 de 7.5, de severidad alta.

Use-After-Free (UAF) es una vulnerabilidad relacionada con el uso incorrecto de la memoria dinámica durante la operación del programa. Si después de liberar una ubicación de memoria, un programa no borra el puntero a esa ubicación, un atacante puede usar el error para comprometer el programa. Puede derivar en denegación de servicio, filtración de memoria e incluso ejecución de código.

Una vulnerabilidad de Use After Free en FortiManager y FortiAnalyzer en el demonio fgfmsd puede permitir que un atacante remoto no autenticado ejecute código no autorizado como root mediante el envío de una solicitud específicamente diseñada al puerto fgfm del dispositivo objetivo.

Se debe tener en cuenta que FGFM está deshabilitado de forma predeterminada en FortiAnalyzer y solo se puede habilitar en modelos de hardware específicos:1000D, 1000E, 2000E, 3000D, 3000E, 3000F, 3500E, 3500F, 3700F, 3900E.

Impacto:

La explotación exitosa de la vulnerabilidad podría permitir a los atacantes remotos no autenticados ejecutar códigos no autorizados/maliciosos como root.

Solución:

Se recomienda a los usuarios actualizar FortiManager y FortiAnalyzer a la última versión disponible en su sitio web oficial.

Mitigación:

- Deshabilite las funciones de FortiManager en la unidad FortiAnalyzer usando el siguiente comando:

```
config system global
set fmg-status disable <--- Desactivado por defecto.
end
```

- Actualice las definiciones de IPS versión 18.100 o superior y asegúrese de que la acción para la firma FG-VD-50483 esté configurada para bloquear.

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-21-067