CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

# Vulnerabilidad de Software

Fecha: 04/11/2022

Problemática: Múltiples Vulnerabilidades en Productos Fortinet

Correlativo: AA-0069

Institución / Sector: Instituciones Públicas y Privadas

## CONTEXTO

Fortinet emitió un comunicado a través de sus canales oficiales para informar a sus usuarios sobre múltiples vulnerabilidades identificadas como CVE-2022-26122, CVE-2022-30307, CVE-2022-35842, CVE-2022-38380 que afectan a sus productos. La explotación exitosa de estas fallas podría llevar a un atacante a ejecutar código arbitrario en el sistema objetivo.

## SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, las fallas encontradas en productos FortiOS afectan a las funciones "RSA SSH", "Read-Only", "AV Engine" y "Telnet on the SSL-VPN interface". Un atacante remoto podría explotar algunas de estas vulnerabilidades para desencadenar la divulgación de información confidencial, la manipulación de datos y eludir las restricciones de seguridad en el sistema objetivo.

Recursos afectados:

FortiOS con motor AV versión 6.2.168 e inferior.

- FortiOS con motor AV versión 6.4.274 e inferior.
- FortiMail con motor AV versión 6.2.168 e inferior.
- FortiMail con motor AV versión 6.4.274 e inferior.
- FortiClient ejecuta el motor AV versión 6.2.168 e inferior.
- FortiClient que ejecuta el motor AV versión 6.4.274 e inferior.
- FortiOS versión 7.2.0
- FortiOS versión 7.0.0 a 7.0.6
- FortiOS versión 6.4.0 a 6.4.9

## Nivel de priorización

| Prioridad<br>Urgente / No Urgente | Actualización<br>Seguimiento/Preventiva/Resiliente |
|---|---|
| **Urgente** | **Preventiva** |

## Matriz de Evaluación

| Riesgo<br>Alto/ Medio/ Bajo | Nivel de Afectación | | |
|---|---|---|---|
| | Integridad | Disponibilidad | Confidencialidad |
| **Alto** | **Alta** | **Alta** | **Alta** |

## RECOMENDACIONES

- Fortinet recomienda encarecidamente a sus usuarios ejecutar las actualizaciones que correspondan para cada uno de los componentes afectados.
- Siga las recomendaciones dadas por el fabricante para mitigar las fallas encontradas, para ello se le invita a visitar los links descritos en la sección de "Referencias".
- Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación.

## DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo y filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).
- Código Arbitrario (RCE): Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.

## REFERENCIAS


1. https://nvd.nist.gov/vuln/detail/CVE-2022-35842
2. https://fortiguard.fortinet.com/psirt/FG-IR-22-228
3. https://fortiguard.fortinet.com/psirt/FG-IR-22-174
4. https://fortiguard.fortinet.com/psirt/FG-IR-22-074
5. https://fortiguard.fortinet.com/psirt/FG-IR-22-223
6. https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities_20221103


ÁREA PARA DEFINICIONES


*La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.