DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°061**	**Fecha: 11-03-2024**
		Página: 7 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en Fortinet FortiOS		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Fortinet ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo escritura fuera de límites que afecta a varios de sus productos y que viene siendo explotado activamente en su naturaleza por diversos actores de amenazas. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios mediante solicitudes HTTP especialmente diseñadas.

2. DETALLES:

La empresa especializada en seguridad informática Fortinet, ha indicado en su boletín mensual que la vulnerabilidad identificada como CVE-2024-21762 podría estar siendo explotada activamente en su naturaleza por diversos actores de amenazas. La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-21762 de tipo escritura fuera de límites en Fortinet FortiOS y FortiProxy, podría permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios mediante solicitudes HTTP especialmente diseñadas.

La empresa indico que ha observado un aumento en la venta de accesos a empresas a través de las VPN de Fortinet en la Deep y Dark web. Estiman que alrededor de 50 mil dispositivos en la región podrían estar afectados por esta vulnerabilidad. Además, la Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) ha informado que la vulnerabilidad está siendo activamente explotada.

Asimismo, según el informe de la organización de seguridad "Shadowserver", se ha identificado numerosos PoC, exploits y herramientas de detección relacionadas con esta vulnerabilidad. De acuerdo con el informe, esta vulnerabilidad afecta a más de 150,000 dispositivos en todo el mundo.

A. Productos afectados:

- FortiOS 7.4 desde 7.4.0 hasta 7.4.2.
- FortiOS 7.2 desde 7.2.0 hasta 7.2.6.
- FortiOS 7.0 desde 7.0.0 hasta 7.0.13.
- FortiOS 6.4 desde 6.4.0 hasta 6.4.14.
- FortiOS 6.2 desde 6.2.0 hasta 6.2.15.
- FortiOS 6.0 todas las versiones.
- FortiProxy 7.4, versión 7.4.0 a 7.4.2.
- FortiProxy 7.2, versión 7.2.0 a 7.2.8.
- FortiProxy 7.0, versión 7.0.0 a 7.0.14.
- FortiProxy 2.0, versión 2.0.0 a 2.0.13.
- FortiProxy 1.2, 1.2 todas las versiones (migrar a una versión fija).
- FortiProxy 1.0, 1.0, 1.1, 1.1 todas las versiones (migrar a una versión fija).

3. RECOMENDACIONES:

- Probar las actualizaciones en entornos no productivos previo al paso a producción.
- Aplicar los parches correspondientes a las vulnerabilidades a la brevedad.
- Desactivar SSL VPN (desactivar el modo web no es una solución válida).

Fuente de Información:	• hxxps://fortiguard.fortinet.com/psirt • hxxps://fortiguard.fortinet.com/psirt/FG-IR-24-015 • hxxps://github.com/BishopFox/cve-2024-21762-check • hxxps://www.bleepingcomputer.com/news/security/critical-fortinet-flaw-may-impact-150-000-exposed-devices/