Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°035	Fecha: 09-02-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	FortiOS y FortiProxy: Múltiples Vulnerabilidades en Fortinet		
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 informado de 3 vulnerabilidades, 2 críticas y 1 media, que afectan a su sistema operativo FortiOS, una de ellas reportada por Gwendal Guégniaud (CVE-2024-23113). La explotación de éstas podría permitir a un atacante ejecutar código o comandos no autorizados.

2. **DETALLES:**

Esta vulnerabilidad de escritura fuera de límites en sslvpnd podría permitir a un atacante remoto, no autenticado, ejecutar código o comandos arbitrarios a través de peticiones HTTP especialmente diseñadas. Se ha asignado el identificador CVE-2024-21762 para esta vulnerabilidad.

Una vulnerabilidad en el uso de cadenas de formato controladas externamente en el demonio fgfmd podría permitir a un atacante remoto, no autenticado, ejecutar código arbitrario o comandos a través de peticiones especialmente diseñadas. Se ha asignado el identificador CVE-2024-23113 para esta vulnerabilidad.

La vulnerabilidad enumerada como CVE-2023-44487 corresponde a un HTTP/2 Rapid Reset Attack. El protocolo HTTP/2 permite una denegación de servicio (consumo de recursos del servidor) porque la cancelación de solicitudes puede restablecer muchas transmisiones rápidamente.

Actualmente se conoce que la vulnerabilidad CVE-2024-21762 está siendo potencialmente explotada. Sin embargo, se desconoce la disponibilidad de exploits que aprovechen estas vulnerabilidades, así como tampoco se han publicado pruebas de concepto (PoC) sobre los detalles del fallo publicado.

Recursos Afectados:

Las siguientes versiones de FortiOS están afectadas:

- FortiOS desde 7.4.0 hasta 7.4.2.
- FortiOS desde 7.2.0 hasta 7.2.6.
- FortiOS desde 7.0.0 hasta 7.0.13.
- FortiOS desde 6.4.0 hasta 6.4.14.
- FortiOS desde 6.2.0 hasta 6.2.15.
- FortiOS todas las versiones 6.0.

Las siguientes versiones de FortiProxy están afectadas:

- Fortiproxy desde 7.4.0 a 7.4.1.
- Fortiproxy desde 7.2.0 a 7.2.7.
- Fortiproxy desde 7.0 todas las versiones.

3. RECOMENDACIONES:

- Actualizar a FortiOS versión 7.4.3 o superior (para las versiones desde 7.4.0 hasta 7.4.2).
- Actualizar a FortiOS versión 7.2.7 o superior (para las versiones desde 7.2.0 hasta 7.2.6).
- Actualizar a FortiOS versión 7.0.14 o superior (para las versiones desde 7.0.0 hasta 7.0.13).
- Actualizar a FortiOS versión 6.4.15 o superior (para las versiones desde 6.4.0 hasta 6.4.14).
- Actualizar a FortiOS versión6.2.16 o superior (para las versiones desde 6.2.0 hasta 6.2.15).
- Migrar a una versión fija (para todas las versiones 6.0 de FortiOS).
- Actualice a Fortiproxy versión 7.4.2 o superior (para las versiones desde 7.4.0 a 7.4.1).
- Actualice a Fortiproxy versión 7.2.8 o superior (para las versiones desde 7.2.0 a 7.2.7)
- Migrar a una versión fija (para todas las versiones 7.0 de FortiProxy).
- Deshabilitar SSL VPN en caso no pueda aplicar los parches (deshabilitar el modo web NO es una solución alternativa válida).
- Eliminar la compatibilidad con HTTP/2 con modo proxy con inspección SSL.

Fuente de Información:	• hxxps://www.fortiguard.com/psirt/FG-IR-24-015 • hxxps://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-fortios-de-fortinet • hxxps://www.ccn-cert.cni.es/es/seguridad-al-dia/avisos-ccn-cert/12896-ccn-cert-av-02-24-actualizaciones-de-seguridad-para-productos-fortinet.html • hxxps://www.fortiguard.com/psirt/FG-IR-23-397