DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 105**	**Fecha: 05-05-2023**
		Página 7 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en FortiOS y FortiProxy sslvpnd		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo escritura fuera de límites en productos Fortios y FortiProxy sslvpnd. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código o comandos no autorizados y comprometer el sistema vulnerable.

2. **Detalles:**

- El software escribe datos más allá del final, o antes del comienzo, del búfer previsto. Esto suele ocurrir cuando el puntero o su índice se incrementa o reduce a una posición más allá de los límites del búfer o cuando la aritmética del puntero da como resultado una posición fuera de la ubicación de memoria válida, por nombrar algunos. Esto puede provocar la corrupción de información confidencial, un bloqueo o la ejecución de código, entre otras cosas.

- La vulnerabilidad registrada con el código CVE-2023-22640 de severidad **alta,** de tipo escritura fuera de límites, existe debido a un error de límite en sslvpnd. Un usuario remoto autenticado puede enviar una solicitud especialmente diseñada para activar una escritura fuera de los límites y ejecutar código arbitrario en el sistema de destino.

3. **Productos afectados:**

- FortiOS versión 7.2.0 a 7.2.3;
- FortiOS versión 7.0.0 a 7.0.10;
- FortiOS versión 6.4.0 a 6.4.11;
- FortiOS versión 6.2.0 a 6.2.13;
- FortiOS 6.0 todas las versiones;
- FortiProxy versión 7.2.0 a 7.2.1;
- FortiProxy versión 7.0.0 a 7.0.7;
- FortiProxy todas las versiones 2.0, 1.2, 1.1, 1.0.

4. **Solución:**

- Fortinet recomienda actualizar los productos afectados con la última versión de software disponible que corrige esta vulnerabilidad:
  - Actualice a FortiOS versión 7.4.0 o superior;
  - Actualice a FortiOS versión 7.2.4 o superior;
  - Actualice a FortiOS versión 7.0.11 o superior;
  - Actualice a FortiOS versión 6.4.12 o superior;
  - Actualice a FortiOS versión 6.2.14 o superior;
  - Actualice a FortiProxy versión 7.2.2 o superior;
  - Actualice a FortiProxy versión 7.0.8 o superior.

- Como solución alterna, se recomienda deshabilitar la opción "Comprobación de host", "Restringir a versiones específicas del sistema operativo" y "Comprobación de host de dirección MAC" en la configuración del portal sslvpn.

Fuentes de información	▪ hxxp://fortiguard.com/psirt/FG-IR-22-475