	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 045	Fecha: 21-02-2023
		Página 7 de 13

Componente que reporta	**CENTRO DE OPERACIONES CIBERESPACIALES**		
Nombre de la alerta	Actualización de Fortinet disponible.		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

SITUACIÓN:

- Se tomó conocimiento que la compañía Fortinet ha lanzado actualizaciones de seguridad para hacer frente a 40 vulnerabilidades en su línea de software, incluidos Fortiweb, FortiOS, FortiProxy y FortiNAC.

DETALLES:

- De las 40 vulnerabilidades 02 tienen calificación crítica, 15 tienen calificación alta, 22 tienen calificación media y 01 tiene gravedad baja.

- La primera de las vulnerabilidades críticas, es un error grave que reside en la solución de acceso a la red FortiNAC (CVE-2022-39952), que podría conducir a la ejecución de un código arbitrario, los productos afectados son los siguientes:

  - FortiNAC versión 9.4.0
  - FortiNAC versión 9.2.0 a 9.2.5
  - FortiNAC versión 9.1.0 a 9.1.7
  - FortiNAC 8.8 todas las versiones
  - FortiNAC 8.7 todas las versiones
  - FortiNAC 8.6 todas las versiones
  - FortiNAC 8.5 todas las versiones
  - FortiNAC 8.3 todas las versiones

- La segunda de las vulnerabilidades críticas es un conjunto de desbordamiento de búfer basado en la pila en el dominio proxy de FortiWeb (CVE-2021-42756), que podría permitir que un atacante remoto no autenticado logre la ejecución de código arbitrario a través de solicitudes HTTP específicamente diseñadas, los productos afectados son los siguientes:

  - FortiWeb versiones 6.4 todas las versiones
  - FortiWeb versiones 6.3.16 y anteriores

- FortiWeb versiones 6.2.6 y anteriores
- FortiWeb versiones 6.1.2 y anteriores
- FortiWeb versiones 6.0.7 y anteriores, y
- FortiWeb versiones 5.x todas las versiones

RECOMENDACIONES

- Actualizar Verificar si cuenta con los productos antes mencionados; de ser así, realizar la actualización de las mismas.
- Realizar la protección de los equipos y sistemas, asegurándose de que estas se encuentren actualizadas, con los parches de seguridad y de contar con un antivirus adecuado.

Fuentes de información	▪ hxxps://thehackernews.com/2023/02/fortinet-issues-patches-for-40-flaws.html