DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 091**	**Fecha: 18-04-2023**
		Página 26 de 33

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Fortinet parchea vulnerabilidad crítica en el servidor de infraestructura local de FortiPresence		
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:**

   Fortinet indico que ha lanzado un parche de seguridad que corrige una vulnerabilidad de severidad **CRÍTICA** de tipo control de acceso inadecuado en la solución de análisis de datos FortiPresence. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso a las instancias de Redis y MongoDB a través de solicitudes de autenticación manipuladas.

2. **Detalles:**

   - Fortinet anunció el lanzamiento de actualizaciones de seguridad en varios de sus productos, incluidos parches para una vulnerabilidad crítica de autenticación faltante en el servidor de infraestructura de FortiPresence que puede explotarse para acceder a las instancias de Redis y MongoDB.
   - FortiPresence es una solución de análisis de datos disponible como un servicio de nube alojado o como una máquina virtual, para instalaciones privadas.
   - La vulnerabilidad registrada con el código CVE-2022-41331 podría permitir que un atacante remoto no autenticado acceda a las instancias de Redis y MongoDB a través de solicitudes de autenticación manipuladas.
   - Por otro lado, Fortinet lanzó también parches para múltiples fallas de alta gravedad en FortiOS, FortiProxy, FortiSandbox, FortiDeceptor, FortiWeb, FortiClient para Windows y macOS, FortiSOAR, FortiADC, FortiDDoS, FortiDDoS-F, FortiAnalyzer y FortiManager.

3. **Productos afectados:**

   - FortiPresence 1.2 todas las versiones;
   - FortiPresence 1.1 todas las versiones;
   - FortiPresence 1.0 todas las versiones.

4. **Solución:**

   - Fortinet recomienda actualizar el producto afectado con la última versión de software disponible que corrige esta vulnerabilidad.

Fuentes de información	▪ hxxps://www.securityweek.com/fortinet-patches-critical-vulnerability-in-data-analytics-solution/ ▪ hxxps://www.fortiguard.com/psirt-monthly-advisory/april-2023-vulnerability-advisories ▪ hxxps://www.fortiguard.com/psirt/FG-IR-22-355