Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 059	Fecha: 09-03-2023
		Página 4 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades en productos de Fortinet		
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

Se ha detectado múltiples vulnerabilidades en productos de Fortinet.

ANTECEDENTES:

- Fortinet es el proveedor mundial en dispositivos de seguridad de red y líder en gestión unificada de amenazas (UTM). Sus productos y servicios ofrecen una gran protección integrada y de alto rendimiento contra las amenazas de seguridad.

DETALLES:

- Fortinet ha publicado 15 avisos de seguridad, un (01) aviso de severidad crítica, cinco (05) altos, ocho (08) medios y uno (01) bajo. La vulnerabilidad crítica podría permitir a un atacante la ejecución de código remoto y/o la realización de una denegación de servicio (DoS), afectando la únicamente un listado en concreto. Productos afectados por la vulnerabilidad de severidad crítica:

  FortiOS, versiones:
  - Desde 7.2.0 hasta 7.2.3.
  - Desde 7.0.0 hasta 7.0.9.
  - Desde 6.4.0 hasta 6.4.11.
  - Desde 6.2.0 hasta 6.2.12.
  - Todas las versiones 6.0.

  FortiProxy, versiones:
  - Desde 7.2.0 hasta 7.2.2.
  - Desde 7.0.0 hasta 7.0.8.
  - Desde 2.0.0 hasta 2.0.11.
  - Todas las versiones 1.2.
  - Todas las versiones 1.1.

- Incluso cuando se ejecuta una versión vulnerable de FortiOS, los dispositivos de hardware que se enumeran a continuación solo se ven afectados por DoS, no por la ejecución de código arbitrario (los dispositivos que no figuran en la lista son vulnerables a ambos):
  - FortiGateRugged-100C
  - FortiGate-100D
  - FortiGate-200C
  - FortiGate-200D
  - FortiGate-300C
  - FortiGate-3600A
  - FortiGate-5001FA2
  - FortiGate-5002FB2
  - FortiGate-60D
  - FortiGate-620B
  - FortiGate-621B
  - FortiGate-60D-POE
  - FortiWiFi-60D
  - FortiWiFi-60D-POE
  - FortiGate-300C-Gen2
  - FortiGate-300C-DC-Gen2

- FortiGate-300C-LENC-Gen2
- FortiWiFi-60D-3G4G-VZW
- FortiGate-60DH
- FortiWiFi-60DH
- FortiGateRugged-60D
- FortiGate-VM01-Hyper-V
- FortiGate-VM01-KVM
- FortiWiFi-60D-I
- FortiGate-60D-Gen2
- FortiWiFi-60D-J
- FortiGate-60D-3G4G-VZW
- FortiWifi-60D-Gen2
- FortiWifi-60D-Gen2-J
- FortiWiFi-60D-T
- FortiGateRugged-90D
- FortiWifi-60D-Gen2-U
- FortiGate-50E
- FortiWiFi-50E
- FortiGate-51E
- FortiWiFi-51E
- FortiWiFi-50E-2R
- FortiGate-52E
- FortiGate-40F
- FortiWiFi-40F
- FortiGate-40F-3G4G
- FortiWiFi-40F-3G4G
- FortiGate-40F-3G4G-NA
- FortiGate-40F-3G4G-EA
- FortiGate-40F-3G4G-JP
- FortiWiFi-40F-3G4G-NA
- FortiWiFi-40F-3G4G-EA
- FortiWiFi-40F-3G4G-JP
- FortiGate-40F-Gen2
- FortiWiFi-40F-Gen2

- La vulnerabilidad de severidad crítica ha sido registrada con el siguiente código CVE-2023-25610.

- Las vulnerabilidades de severidad alta han sido registradas con los siguientes códigos CVE-2022-42476, CVE-2023-25605, CVE-2022-39951, CVE-2022-40676, CVE-2022-39953.

- Las vulnerabilidades de severidad media han sido registradas con los siguientes códigos CVE-2022-45861, CVE-2022-41329, CVE-2023-25611, CVE-2022-41333, CVE-2023-23776, CVE-2022-22297, CVE-2022-41328, CVE-2022-27490.

- La vulnerabilidad de severidad baja ha sido registrada con el siguiente código CVE-2022-29056.

RECOMENDACIONES:

- Aculalizar FortiOS a la versión 7.4.0 o superior.
- Aculalizar FortiOS a la versión 7.2.4 o superior.
- Aculalizar FortiOS a la versión 7.0.10 o superior.
- Aculalizar FortiOS a la versión 6.4.12 o superior.
- Aculalizar FortiOS a la versión 6.2.13 o superior.
- Aculalizar FortiProxy a la versión 7.2.3 o superior.
- Aculalizar FortiProxy a la versión 7.0.9 o superior.
- Aculalizar FortiProxy a la versión 2.0.12 o superior.
- Aculalizar FortiOS-6K7K a la versión 7.0.10 o superior.
- Aculalizar FortiOS-6K7K a la versión 6.4.12 o superior.
- Aculalizar FortiOS-6K7K a la versión 6.2.13 o superior.

- Se recomienda realizar una copia de seguridad de la configuración de los equipos y/o tener la capacidad de realizar un RoollBack para cualquier incidente que se pueda derivar por la actualización.

- De no poder realizar la actualización, como alternativa, deshabilitar la interfaz administrativa HTTP/HTTPS o Limite las direcciones IP que pueden llegar a la interfaz administrativa, el procedimiento para limitar las direcciones IP lo puede encontrar en el aviso de Fortinet.

- Para las vulnerabilidades de severidad alta, media y baja, realizar la consulta de las actualizaciones disponibles en el aviso de seguridad de Fortinet.

Fuentes de información	▪ hxxps:// www.fortiguard.com/psirt/FG-IR-23-001 ▪ hxxps://www.fortiguard.com/psirt-monthly-advisory/march-2023-vulnerability-advisories ▪ Análisis propio de fuentes abiertas.