Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 065	Fecha: 16-03-2023 Página 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Defecto de Fortinet FortiOS explotado en ciberataques dirigidos a entidades gubernamentales		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet, Redes Sociales, Correo Electrónico		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

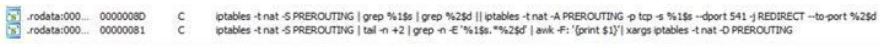
Las entidades gubernamentales y las grandes organizaciones han sido atacadas por un actor de amenazas desconocido al explotar una falla de seguridad en el software Fortinet FortiOS para provocar la pérdida de datos y la corrupción del sistema operativo y los archivos.

DETALLES:

- La falla de día cero en cuestión es CVE-2022-41328 (puntaje CVSS: 6.5), una falla transversal de ruta de seguridad media en FortiOS que podría conducir a la ejecución de código arbitrario.
- Una limitación inapropiada de un nombre de ruta a una vulnerabilidad de directorio restringido ('path traversal') [CWE-22] en FortiOS puede permitir que un atacante privilegiado lea y escriba archivos arbitrarios a través de comandos CLI manipulado.
- La deficiencia afecta a las versiones 6.0, 6.2, 6.4.0 a 6.4.11, 7.0.0 a 7.0.9 y 7.2.0 a 7.2.3 de FortiOS. Las correcciones están disponibles en las versiones 6.4.12, 7.0.10 y 7.2.4 respectivamente.
- La divulgación se produce días después de que Fortinet lanzara parches para abordar 15 fallas de seguridad, incluido CVE-2022-41328 y un problema crítico de subdesbordamiento de búfer basado en montón que afecta a FortiOS y FortiProxy (CVE-2023-25610, puntaje CVSS: 9.3).
- El defecto de seguridad salió a la luz, según la compañía con sede en Sunnyvale, después de que varios dispositivos FortiGate pertenecientes a un cliente anónimo sufrieron una "detención repentina del sistema y una falla posterior en el arranque", lo que indica una violación de la integridad.

File Path	MD5	Notes
/bin/auth	b6e92149efaf78e9ce7552297505b9d5	Not present in clean FMG
/bin/klogd	53a69adac914808eced2bf8155a7512d	Not present in clean FMG
/bin/support	9ce2459168cf4b5af494776a70e0feda	Not present in clean FMG
/etc/init.d/localnet	88711ebc99e1390f1ce2f42a6de0654d	Modified
/usr/local/lib/python3.8/proj/urls.py	64bdf7a631bc76b01b985f1d46b35ea6	Modified
/usr/local/lib/python3.8/proj/views.py	3e43511c4f7f551290292394c4e21de7	Modified

File path	/rootfs.gz/rootfs/bin/auth
MD5	b6e92149efaf78e9ce7552297505b9d5
File type	ELF 64-bit LSB executable, x86-64, statically linked, stripped
File timestamp (GMT-4)	Sept 27, 2022 08:54:00



File path	/rootfs.gz/rootfs/usr/local/lib/python3.8/proj/util/urls.py
MD5	64bdf7a631bc76b01b985f1d46b35ea6
File type	Python script
File timestamp (GMT-4)	Sept 27, 2022 08:54:00

File path	/rootfs.gz/rootfs/usr/local/lib/python3.8/proj/util/views.py
MD5	3e43511c4f7f551290292394c4e21de7
File type	Python script
File timestamp (GMT-4)	Sept 27, 2022 08:54:00

- Un análisis más detallado del incidente reveló que los actores de la amenaza modificaron la imagen del firmware del dispositivo para incluir una nueva carga útil ("/bin/fgfm") de modo que siempre se inicie antes de que comience el proceso de arranque.

- El malware /bin/fgfm está diseñado para establecer contacto con un servidor remoto para descargar archivos, extraer datos del host comprometido y otorgar acceso de shell remoto.

- Se dice que los cambios adicionales introducidos en el firmware proporcionaron al atacante acceso y control persistentes, sin mencionar incluso la desactivación de la verificación del firmware al inicio.

- Fortinet dijo que el ataque fue altamente dirigido, con evidencia que apunta a organizaciones gubernamentales o afiliadas al gobierno.

- Dada la complejidad del exploit, se sospecha que el atacante tiene un "conocimiento profundo de FortiOS y el hardware subyacente" y posee capacidades avanzadas para realizar ingeniería inversa en diferentes aspectos del sistema operativo FortiOS.

RECOMENDACIONES:

- Actualizar a las versiones 6.4.12, 7.0.10 y 7.2.4 de FortiOS.
- Mantener actualizada los software (Sistema operativo y antivirus) de las estaciones de trabajo.

Fuentes de información	▪ https://thehackernews.com/2023/03/fortinet-fortios-flaw-exploited-in.html ▪ Análisis propio de fuentes abiertas.