Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTIOS: FORTIOS / FORTIPROXY – HEAP BUFFER UNDERFLOW DETECTADO EN LA INTERFAZ ADMINISTRATIVA

09 /Enero/2023

CONTENIDO

INTRODUCCIÓN

Una vulnerabilidad de escritura de búfer (‘buffer underflow’) en la interfaz administrativa de FortiOS y FortiProxy podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el dispositivo y / o realizar un DoS en la GUI, mediante solicitudes específicamente diseñadas.

HEAP BUFFER UNDERFLOW DETECTADO EN LA INTERFAZ ADMINISTRATIVA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_03_09_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Medio
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/12/2022
Es día cero (0 day):	No

RESUMEN

Una vulnerabilidad de escritura de búfer (‘buffer underflow’) en la interfaz administrativa de FortiOS y FortiProxy podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el dispositivo y / o realizar un DoS en la GUI, mediante solicitudes específicamente diseñadas.

Estado de explotación:
Fortinet no tiene conocimiento de ninguna instancia en la que se haya explotado esta vulnerabilidad en el mundo real. ‘Revisamos y probamos continuamente la seguridad de nuestros productos, y esta vulnerabilidad fue descubierta internamente dentro de ese marco’ dijo Fortinet.

Productos afectados

- FortiOS versión 7.2.0 hasta 7.2.3
- FortiOS versión 7.0.0 hasta 7.0.9
- FortiOS versión 6.4.0 hasta 6.4.11
- FortiOS versión 6.2.0 hasta 6.2.12
- FortiOS 6.0 todas las versiones

- FortiProxy versión 7.2.0 hasta 7.2.2
- FortiProxy versión 7.0.0 hasta 7.0.8
- FortiProxy versión 2.0.0 hasta 2.0.11
- FortiProxy 1.2 todas las versiones
- FortiProxy 1.1 todas las versiones

Incluso cuando se ejecuta una versión vulnerable de FortiOS, los dispositivos de hardware enumerados a continuación se ven afectados solo por la parte de DoS del problema, no por la ejecución de código arbitrario (los dispositivos no enumerados son vulnerables a ambas cosas):

- 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

Solución

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

RECOMENDACIONES

- Realizar la actualización de sus equipos para evitar esta y otras vulnerabilidades que puedan ser explotadas en los mismos.
- Desactivar la interfaz administrativa HTTP/HTTPS o limitar las direcciones IP que pueden acceder a la interfaz administrativa

NOTICIA COMPLETA

https://devel.group/blog/fortios-fortiproxy-heap-buffer-underflow-en-la-interfaz-administrativa/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente