Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTIOS: DESBORDAMIENTO DE BÚFER BASADO EN SSLVPND

12 /Diciembre/2022

CONTENIDO

INTRODUCCIÓN

Fortinet emitió el lunes un parche de emergencia para cubrir una vulnerabilidad grave en su producto FortiOS SSL-VPN, advirtiendo que los piratas informáticos ya han explotado la falla en la naturaleza.

DESBORDAMIENTO DE BÚFER BASADO EN SSLVPND

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

ID de alerta:	DSOC-CERT_2022_12_12_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

Fortinet emitió el lunes un parche de emergencia para cubrir una vulnerabilidad grave en su producto FortiOS SSL-VPN, advirtiendo que los piratas informáticos ya han explotado la falla en la naturaleza.

Un aviso de nivel crítico de Fortinet describió el error como una corrupción de memoria que permite a un "atacante remoto no autenticado" lanzar código dañino o ejecutar comandos en un sistema objetivo.

"Una vulnerabilidad de desbordamiento de búfer basada en montón [CWE-122] en FortiOS SSL-VPN puede permitir que un atacante remoto no autenticado ejecute código arbitrario o comandos a través de solicitudes específicamente diseñadas", advirtió la compañía.

Estado de explotación:
Fortinet es consciente de una instancia en la que esta vulnerabilidad fue explotada, y recomienda validar inmediatamente sus sistemas contra los siguientes indicadores de compromiso:

Multiples entradas de registro con:
Logdesc=”Application crashed” and msg=”[…] application:sslvpnd,[…], Signal 11 received, Backtrace: […]“

Presencia de los siguientes artefactos en el sistema de archivos:

- /data/lib/libips.bak
- /data/lib/libgif.so
- /data/lib/libiptcp.so
- /data/lib/libipudp.so
- /data/lib/libjepg.so
- /var/.sslvpnconfigbk
- /data/etc/wxd.conf
- /flash

Conexiones a direcciones IP sospechosas desde FortiGate:

- 188.34.130.40:444
- 103.131.189.143:30080,30081,30443,20443
- 192.36.119.61:8443,444
- 172.247.168.153:8033

Productos afectados:

- FortiOS versión 7.2.0 a 7.2.2
- FortiOS versión 7.0.0 a 7.0.8
- FortiOS versión 6.4.0 a 6.4.10
- FortiOS versión 6.2.0 a 6.2.11
- FortiOS-6K7K versión 7.0.0 a 7.0.7
- FortiOS-6K7K versión 6.4.0 a 6.4.9
- FortiOS-6K7K versión 6.2.0 a 6.2.11
- FortiOS-6K7K versión 6.0.0 a 6.0.14

Soluciones

- Actualice a FortiOS versión 7.2.3 o superior
- Actualice a FortiOS versión 7.0.9 o superior
- Actualice a FortiOS versión 6.4.11 o superior
- Actualice a FortiOS versión 6.2.12 o superior
- Actualice a FortiOS-6K7K versión 7.0.8 o superior
- Actualice a FortiOS-6K7K versión 6.4.10 o superior
- Actualice a FortiOS-6K7K versión 6.2.12 o superior
- Actualice a FortiOS-6K7K versión 6.0.15 o superior

RECOMENDACIONES

- Validar las conexiones hacia las direcciones IP sospechosas desde FortiGate.

- Realizar la actualización de sus equipos para evitar esta y otras vulnerabilidades que puedan ser explotadas en los mismos.

NOTICIA COMPLETA

https://devel.group/blog/fortios-desbordamiento-de-bufer-basado-en-sslvpnd/

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