Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Fortinet pide actualizar FortiOS/FortiProxy debido a bugs en inicios de sesión.

10/Octubre/2022

Contenido

INTRODUCCIÓN

Fortinet ha advertido a los administradores que actualicen los firewalls FortiGate y los servidores proxy web FortiProxy a las últimas versiones, que abordan una vulnerabilidad de gravedad crítica.

VULNERABILIDAD CRITICA EN FORTIOS

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

ID de alerta:	DSOC-CERT_2022_10_09_01
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/10/2022
Es día cero (0 day):	No

RESUMEN

La falla de seguridad (rastreada como CVE-2022-40684) es una omisión de autenticación en la interfaz administrativa que podría permitir que los actores de amenazas remotos inicien sesión en dispositivos sin parches.

"Una omisión de autenticación utilizando una ruta o canal alternativo en FortiOS y FortiProxy puede permitir que un atacante no autenticado realice operaciones en la interfaz administrativa a través de solicitudes HTTP o HTTPS especialmente diseñadas", explica Fortinet.

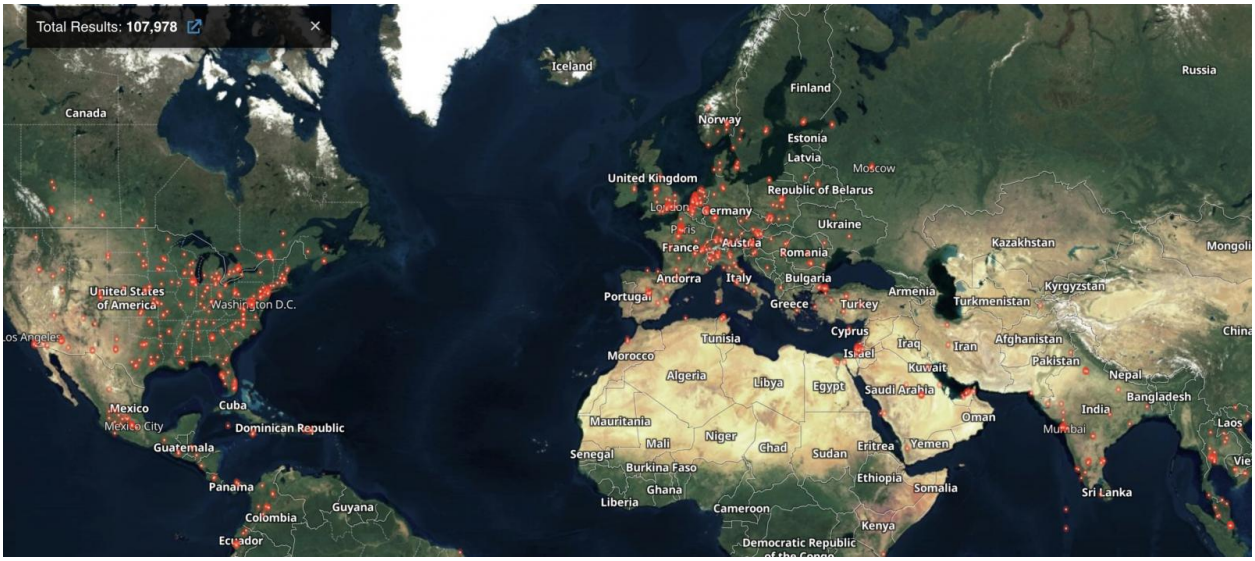
"Esta es una vulnerabilidad crítica y debe tratarse con la máxima urgencia", agrega la compañía.

Fortinet también envió correos electrónicos a los clientes y les aconsejó que actualicen a las últimas versiones disponibles de inmediato.

"Debido a la capacidad de explotar este problema de forma remota, Fortinet recomienda encarecidamente a todos los clientes con las versiones vulnerables que realicen una actualización inmediata", advirtió la compañía .

Según una búsqueda de Shodan , se puede acceder a más de 100,000 firewalls FortiGate desde Internet, aunque se desconoce si sus interfaces de administración también están expuestas.

Cortafuegos FortiGate expuestos a Internet:



La lista completa de productos vulnerables a los ataques que intentan explotar la falla CVE-2022-40684 incluye:

FortiOS: De 7.0.0 a 7.0.6 y de 7.2.0 a 7.2.1

FortiProxy: De 7.0.0 a 7.0.6 y 7.2.0

Solución

Fortinet recomienda aplicar actualizaciones a las versiones vulnerables mostradas en la siguiente tabla:

Producto	Versiones Vulnerables	Versión Segura
FortiOS	7.0.0 a 7.0.6	7.0.7 y 7.2.2
FortiProxy	7.0.0 a 7.0.6 y 7.2.0	7.0.7 y 7.2.1

Si no puede aplicar parches de inmediato, Fortinet establece que usar una política local para limitar el acceso a la interfaz de administración. Fortinet también incluye pasos para deshabilitar el acceso administrativo a la interfaz orientada a Internet y pasos para restringir el acceso a hosts confiables en su Guía de Fortalecimiento de FortiGate. Como señala la guía, estos pasos son parte de las mejores prácticas del administrador del sistema.

RECOMENDACIONES

- Se recomienda actualizar sus dispositivos Fortinet a la brevedad.

- La administración HTTPS mediante internet debe desactivarse inmediatamente y usarse de manera local hasta que se pueda realizar la actualización.

- Si no puede deshabilitar la administración HTTPS desde internet, para evitar que los atacantes remotos eludan la autenticación e inicien sesión en implementaciones vulnerables de FortiGate y FortiProxy, los clientes deben limitar las direcciones IP públicas que pueden llegar a la interfaz administrativa mediante una política local.

Noticia Completa

https://devel.group/blog/vulnerabilidad-encontrada-en-fortios-y-fortiproxy/

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