Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

¡NUEVOS DATOS REVELADOS! LA BRECHA DE SEGURIDAD EN FORTIGATE SIGUE EN ESCALADA

23 / 01 / 2025

CONTENIDO

INTRODUCCIÓN....3
RESUMEN....5
NOTICIA COMPLETA....6
CONTACTOS DE SOPORTE....7

INTRODUCCIÓN

La reciente revelación de nuevas filtraciones masivas en dispositivos FortiGate ha puesto en alerta al mundo de la ciberseguridad. Tras un ataque inicial que ya comprometió credenciales y configuraciones críticas, los atacantes han intensificado sus esfuerzos, exponiendo redes sensibles de instituciones gubernamentales, educativas y grandes corporaciones. Estos eventos subrayan la urgencia de fortalecer la seguridad en dispositivos críticos y adoptar medidas de mitigación para prevenir futuros ataques que podrían afectar gravemente la integridad y confidencialidad de las redes globales.

¡NUEVOS DATOS REVELADOS! LA BRECHA DE SEGURIDAD EN FORTIGATE SIGUE EN ESCALADA

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

ID de alerta:	DSOC-CERT_2025_01_23_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	23/01/2025
Es día cero (0 day):	No

RESUMEN

Hace apenas una semana, el mundo de la ciberseguridad fue sacudido por una filtración masiva de datos que expuso configuraciones y credenciales de más de 15,000 dispositivos FortiGate. Esta noticia alertó a empresas e instituciones en todo el mundo. Detrás de esta brecha se encuentra el grupo de ciberdelincuentes conocido como Belsen Group, quienes aprovecharon una vulnerabilidad crítica en los dispositivos para acceder a información sensible.

En su momento, esta filtración ya había causado una preocupación significativa al permitir que atacantes pudieran acceder a redes internas, robar datos confidenciales e incluso ejecutar ataques más sofisticados. Además, países de Centroamérica y el Caribe, como Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá y República Dominicana, se vieron afectados, demostrando que ninguna región está exenta de estas amenazas. Sin embargo, lo que parecía ser el límite del daño ha escalado aún más con nuevas filtraciones reveladas recientemente.

¡NUEVOS DATOS REVELADOS!

La alarma vuelve a sonar en el mundo de la ciberseguridad. Recientemente se han revelado nuevas filtraciones que afectan a dispositivos FortiGate, intensificando la gravedad del problema inicial que ya había comprometido configuraciones sensibles, certificados y credenciales. Esta vez, la situación se vuelve aún más preocupante, ya que los datos expuestos no solo incluyen configuraciones internas de las redes, sino también listas de dominios asociados a estas configuraciones vulnerables.

Entre los nuevos datos filtrados, se destacan nombres de dominios pertenecientes a redes gubernamentales, instituciones educativas y grandes corporaciones, exponiendo a estas organizaciones a mayores riesgos de ciberataques, como phishing avanzado, robo de identidad y accesos no autorizados a redes internas, afectando aún más la integridad y confidencialidad de las redes vulneradas. Esta evolución evidencia que los atacantes están redoblando esfuerzos para explotar la vulnerabilidad **CVE-2022-40684**, aprovechando el hecho de que muchas organizaciones aún no han aplicado los parches necesarios.

Este incidente resalta la importancia de actuar con urgencia, aplicando las actualizaciones de seguridad necesarias y revisando configuraciones en dispositivos críticos como los FortiGate, para evitar que el impacto de estas filtraciones continúe escalando.

RECOMENDACIONES PARA MITIGAR EL RIESGO

1. **Aplicar los parches de seguridad pendientes:** Asegúrate de instalar las actualizaciones proporcionadas por Fortinet, especialmente las relacionadas con la vulnerabilidad CVE-2022-40684. Esto es crucial para cerrar la brecha que permitió las filtraciones iniciales.
2. **Cambiar credenciales y certificados afectados:** Si no se ha hecho previamente, realiza un cambio inmediato de todas las contraseñas y certificados expuestos. Usa contraseñas únicas, complejas y habilita el uso de autenticación multifactor (MFA).
3. **Monitorear actividad sospechosa:** Implementa sistemas de monitoreo continuo para detectar actividades anómalas, intentos de acceso no autorizado y tráfico inusual en las redes que utilizan dispositivos FortiGate.

4. **Actualizar listas de acceso y dominios permitidos:** Con las listas de dominios expuestos en la filtración, revisa las políticas de acceso, asegurándote de que solo los dominios autorizados tengan permisos para interactuar con tus dispositivos y redes.
5. **Capacitar al personal:** Proporciona formación al equipo encargado de la ciberseguridad para que estén al tanto de las mejores prácticas para gestionar dispositivos críticos como FortiGate y sepan responder rápidamente ante un incidente.
6. **Segmentar las redes:** Implementa una segmentación efectiva de las redes para minimizar el impacto en caso de que un dispositivo comprometido sea explotado. Asegúrate de que los dispositivos críticos estén aislados de segmentos menos seguros.

INDICADORES DE COMPROMISO

NOTICIA COMPLETA

https://devel.group/blog/nuevos-datos-revelados-la-brecha-de-seguridad-en-fortigate-sigue-en-escalada/

CONTACTOS DE SOPORTE

Correo electrónico: info@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/