Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERCRIMINALES FILTRAN DATOS CRÍTICOS DE FORTIGATE: 15,000 DISPOSITIVOS EN RIESGO

17 / 01 / 2025

CONTENIDO

INTRODUCCIÓN

Se aborda un caso de filtración masiva de datos que expuso configuraciones y credenciales de más de 15,000 dispositivos FortiGate, comprometiendo la seguridad de redes empresariales y gubernamentales. Este incidente, atribuido a Belsen Group, se originó por la explotación de una vulnerabilidad en FortiOS que, aunque parchada en 2022, no fue corregida por muchas organizaciones. Lo relevante de esta filtración radica en la publicación estructurada de datos en la dark web, incluyendo direcciones IP, credenciales en texto plano y certificados digitales, facilitando ataques como movimientos laterales, ransomware y espionaje. La falta de medidas de mitigación oportunas subraya la importancia de actualizaciones de seguridad y monitoreo continuo.

CIBERCRIMINALES FILTRAN DATOS CRÍTICOS DE FORTIGATE: 15,000 DISPOSITIVOS EN RIESGO

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

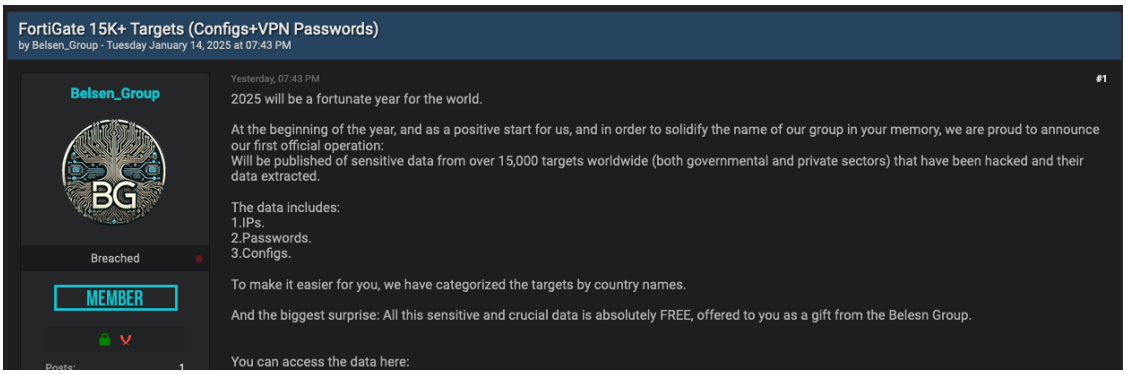
ID de alerta:	DSOC-CERT_2025_01_17_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	17/01/2025
Es día cero (0 day):	No

RESUMEN

Una reciente filtración de datos ha generado gran preocupación en el ámbito de la ciberseguridad. Miles de dispositivos FortiGate, utilizados por empresas e instituciones para proteger sus redes, han quedado expuestos debido a la divulgación de configuraciones y credenciales VPN.

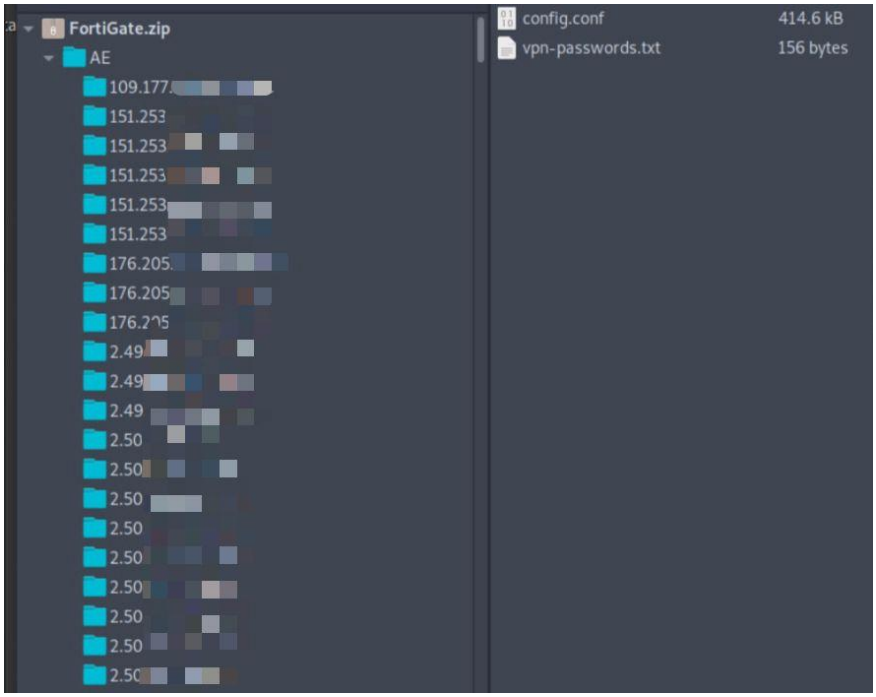
¿Qué pasó?

En los últimos días, la comunidad de ciberseguridad ha sido sacudida por una nueva amenaza: Belsen Group, un actor emergente en el mundo del cibercrimen ha filtrado en la dark web configuraciones y credenciales de más de 15,000 dispositivos FortiGate. Este incidente pone en riesgo la seguridad de miles de empresas y organizaciones alrededor del mundo, ya que expone información crítica que podría ser utilizada para ataques más sofisticados.



El grupo publicó un archivo de 1.6 GB, organizado meticulosamente por país y dirección IP, que contiene datos altamente sensibles como:

- Direcciones IP y configuraciones completas de los dispositivos comprometidos.
- Nombres de usuario y contraseñas, algunas de ellas en texto plano.
- Certificados digitales de administración de dispositivos, lo que podría permitir ataques de intermediario (MitM).
- Reglas de firewall y configuraciones de seguridad, lo que facilita la evasión de medidas de protección.



¿Cómo ocurrió esta filtración?

En octubre de 2022, Fortinet emitió actualizaciones de seguridad para corregir una vulnerabilidad crítica identificada como CVE-2022-40684. Este fallo afectaba a FortiOS, FortiProxy y FortiSwitchManager, permitiendo que atacantes no autenticados obtuvieran acceso con privilegios administrativos a los sistemas comprometidos.

A pesar de las advertencias de Fortinet sobre la urgencia de aplicar estos parches, un gran número de organizaciones no actualizó sus dispositivos a tiempo, lo que dejó miles de sistemas expuestos. Esta falta de actualización permitió que actores malintencionados, como Belsen Group, explotaran la vulnerabilidad y accedieran a configuraciones sensibles y credenciales VPN de los dispositivos FortiGate.

La divulgación de estas credenciales y configuraciones representa una amenaza significativa para empresas y entidades gubernamentales, que dependen de los firewalls FortiGate para proteger sus redes. Ante este escenario, expertos en ciberseguridad están evaluando el impacto de la filtración y sugiriendo medidas urgentes para mitigar posibles ataques, ya que los ciberdelincuentes podrían aprovechar estas brechas para lanzar ataques aún más sofisticados.

¿Qué significa esta filtración para las empresas?

- **Acceder remotamente a los dispositivos comprometidos** y tomar control total de la infraestructura de red.

- **Explotar las credenciales filtradas** para realizar movimientos laterales dentro de las redes internas de las empresas.
- **Desplegar ransomware o instalar puertas traseras** para futuros ataques.
- **Realizar espionaje corporativo o robo de datos confidenciales.**

¿Qué países fueron afectados por la filtración de FortiGate?

El impacto de esta filtración no se limita a grandes potencias tecnológicas; países de Centroamérica y el Caribe también se han visto afectados. Entre las naciones con dispositivos comprometidos se encuentran Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá y República Dominicana, lo que demuestra que ninguna región está exenta de este tipo de amenazas, ya que podría facilitar el acceso indebido a sus redes y abrir la puerta a ciberataques más sofisticados.

Recomendaciones de mitigación

1. **Actualizar el firmware:** Es fundamental instalar la última versión disponible del software para corregir vulnerabilidades críticas. Se recomienda actualizar FortiOS FortiOS (7.0.7 o superior en la rama 7.0 y 7.2.2 o superior en la rama 7.2), FortiProxy (7.0.7 o superior en la rama 7.0 y 7.2.1 o superior en la rama 7.2) y FortiSwitchManager (7.2.1 o superior) Mantener los sistemas actualizados reduce significativamente el riesgo de explotación por parte de atacantes.
2. **Reforzar la seguridad de credenciales**: Cambiar **todas las contraseñas** de acceso y habilitar **autenticación multifactor (MFA)** para evitar accesos no autorizados incluso si las credenciales han sido comprometidas.
3. **Auditar tráfico y registros**: Revisar **logs de actividad** en busca de conexiones sospechosas o intentos de acceso inusuales. Herramientas de detección de intrusos pueden ayudar a identificar anomalías en la red.
4. **Implementar segmentación de red**: Limitar el acceso de dispositivos a información sensible mediante **reglas de acceso más estrictas** y segmentación de red, reduciendo así el impacto de posibles accesos no autorizados.
5. **Monitorear la dark web**: Utilizar herramientas de inteligencia de amenazas para verificar si **credenciales de la empresa han sido filtradas** y tomar acciones preventivas en caso de exposición.

Impacto y Lecciones aprendidas

La filtración de datos de FortiGate por parte de Belsen Group destaca la importancia de mantener los sistemas actualizados y de aplicar medidas de seguridad más allá de los firewalls. Los atacantes adoptaron un enfoque oportunista, aprovechando una vulnerabilidad que, aunque ya tenía parches disponibles, dejó a muchas organizaciones expuestas. Esto subraya la necesidad de aplicar actualizaciones sin demora y de fortalecer las defensas adicionales como la autenticación multifactor y la segmentación de redes.

El incidente también resalta la relevancia de fomentar una cultura de ciberseguridad proactiva. No solo se trata de reaccionar ante incidentes, sino de mantener una vigilancia constante y de anticiparse a las amenazas. Las empresas deben integrar una estrategia de seguridad sólida que incluya no solo tecnología avanzada, sino también capacitación y procedimientos adecuados para minimizar el riesgo de futuros ataques.

NOTICIA COMPLETA

https://devel.group/blog/cibercriminales-filtran-datos-criticos-de-fortigate-15000-dispositivos-en-riesgo/

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/