[Publish] - 8. Forzar el uso de TLS 1.2 para todos los listeners seguros

El hallazgo de seguridad **"Forzar el uso de TLS 1.2 para todos los listeners seguros"** se enfoca en deshabilitar versiones más antiguas y vulnerables de los protocolos de cifrado. Los protocolos **TLS (Transport Layer Security)** 1.0 y 1.1 tienen vulnerabilidades criptográficas conocidas que los hacen susceptibles a ataques como POODLE y BEAST.

Permitir que los clientes se conecten utilizando estos protocolos obsoletos pone en riesgo la confidencialidad e integridad de los datos en tránsito. La mejor práctica de seguridad, y un requisito para muchos estándares de cumplimiento como PCI DSS, es configurar los servidores para que solo acepten conexiones que utilicen protocolos de cifrado fuertes y modernos, como **TLS 1.2** y **TLS 1.3**.

AWS gestiona esto a través de **Políticas de Seguridad (Security Policies)** que se aplican a los listeners HTTPS de los balanceadores de carga.

Análisis de los Listeners Reportados

Los siguientes listeners de balanceadores de carga han sido identificados por utilizar una política de seguridad que aún permite el uso de protocolos TLS obsoletos (1.0 o 1.1).

Tipo	Nombre del Recurso (Listener)	Número de Cuenta
LoadBalancer	listener/app/Colabora/1d5feb4717929008/3384be1888b63b9e	398984081329
LoadBalancer	listener/app/django-lb/30a6513ddc6c110e/78ca2c282d701320	002670977573
LoadBalancer	listener/app/GS-Connection-SAP/fbfa9801af1ba972/12b5a2427a941b58	613703092215
LoadBalancer	listener/app/gs-services/844a3cc33b5de0c7/bbd83a43c7a18843	002670977573

LoadBalancer	listener/app/ServDigitales/392f0dbef015d8d1/811fa4d7af3f9169	890342916428

Preguntas para tu Equipo (Acción Requerida)

La actualización de la política de seguridad puede afectar a clientes muy antiguos que no soporten TLS 1.2.

1. **Compatibilidad de Clientes:** ¿Existe algún requisito conocido de dar soporte a clientes o sistemas operativos muy antiguos (ej. Windows XP, versiones antiguas de Android, navegadores de hace más de 10 años)? La gran mayoría de los clientes modernos soportan TLS 1.2 sin problemas, pero es una pregunta que vale la pena hacer para evitar interrupciones inesperadas.

Consideraciones de Costo

No hay **ningún costo directo** asociado con la actualización de la política de seguridad de un listener en un balanceador de carga. Esta es una configuración de seguridad fundamental proporcionada por AWS sin cargo adicional.

Cómo Solucionarlo: Actualizar la Política de Seguridad del Listener

El proceso para remediar este hallazgo es rápido y se puede hacer sin tiempo de inactividad.

1. **Navegar al Balanceador de Carga:**
   - Ve a la consola de **EC2**.
   - En el panel de navegación izquierdo, en **Carga y Escalado**, elige **Balanceadores de Carga**.
2. **Seleccionar el Listener:**
   - Selecciona el balanceador de carga correspondiente de la lista.
   - Ve a la pestaña **Listeners**.
   - Selecciona el listener **HTTPS:443** que deseas modificar y haz clic en **Editar**.
3. **Actualizar la Política de Seguridad:**
   - En la sección **Protocolo seguro (Secure listener settings)**, encontrarás un menú desplegable para la **Política de seguridad (Security policy)**.
   - La política actual probablemente será una más antigua como `ELBSecurityPolicy-2016-08` o una similar.
   - Selecciona una política moderna que fuerce el uso de TLS 1.2. La política recomendada por AWS es `ELBSecurityPolicy-TLS-1-2-2021-06` o una más reciente. Esta política ofrece un excelente balance entre seguridad y compatibilidad.

- Haz clic en **Guardar cambios**.

4. **Repetir:** Realiza este proceso para todos los listeners HTTPS identificados.

Recomendación

Se recomienda que se actualicen las políticas de seguridad de todos los listeners HTTPS listados a `ELBSecurityPolicy-TLS-1-2-2021-06` o una política más reciente. Este cambio es transparente para la gran mayoría de los usuarios y fortalece significativamente la seguridad de tus aplicaciones al eliminar la compatibilidad con protocolos de cifrado débiles y vulnerables.

Referencias

Security policies for your Application Load Balancer - Elastic Load Balancing