[Publish] - 12. La política del bucket de S3 no debe permitir acciones 'Get' para todos los principales sin una condición

El hallazgo de seguridad **"La política del bucket de S3 no debe permitir acciones 'Get' para todos los principales (Principals) sin una condición"** identifica una configuración de alto riesgo. Específicamente, significa que la política de permisos del bucket contiene una declaración que permite la acción `s3:GetObject` (leer objetos) para un `Principal` de `"*"` (cualquier persona en internet).

Esto convierte efectivamente al bucket en un servidor de archivos público, donde **cualquier persona con el enlace puede descargar los objetos almacenados**. Aunque a veces esto es intencional para alojar sitios web estáticos, es una configuración peligrosa que puede llevar a:

- **Fuga de Datos Sensibles:** Si se carga accidentalmente un archivo incorrecto, queda expuesto de inmediato.
- **Costos Inesperados:** Cualquier persona puede descargar tus archivos repetidamente, lo que puede generar altos costos de transferencia de datos salientes de S3.
- **Exposición de Activos de la Aplicación:** Expone la estructura y los activos de tu frontend, lo que podría dar pistas a un atacante.

La práctica recomendada para servir contenido público es utilizar **Amazon CloudFront**, que actúa como una capa protectora y de caché frente a tu bucket.

Análisis de los Buckets Reportados

Los siguientes buckets de S3 han sido identificados con una política que permite el acceso público de lectura.

Tipo	Nombre del Bucket	Número de Cuenta	Propósito Inferido
S3	`banco-imagen-gs-frontend`	002670977573	Probablemente aloja activos estáticos (imágenes, CSS, JS) para el frontend de una aplicación.

S3	`biometricos-frontend`	002670977573	Similar al anterior, probablemente contiene los archivos del frontend para una aplicación de biométricos.

Observación Clave: Los nombres de ambos buckets sugieren que su propósito es alojar contenido de un sitio web estático. Si bien el contenido debe ser público, permitir el acceso directo al bucket no es la forma más segura ni eficiente de hacerlo.

Preguntas para tu Equipo (Acción Requerida)

Para implementar la solución correcta, por favor coordina con los dueños de las aplicaciones para responder:

1. **Confirmación del Propósito:** ¿Pueden confirmar que estos dos buckets se utilizan para alojar activos de sitios web públicos?
2. **Sensibilidad del Contenido:** ¿Existe algún dato sensible o propietario en estos buckets, o son únicamente activos públicos como imágenes, hojas de estilo y scripts?
3. **Uso Actual:** ¿Cómo acceden los usuarios finales a este contenido actualmente? ¿A través de la URL directa del bucket de S3 o ya existe un dominio personalizado?

Consideraciones de Costo

- **Modificar la Política de Bucket:** Cambiar la política de permisos de un bucket de S3 es **gratuito**.
- **Implementar Amazon CloudFront:**
  - **Transferencia de Datos:** La transferencia de datos desde S3 hacia CloudFront es **gratuita**. Los costos de transferencia de datos de CloudFront hacia los usuarios suelen ser más bajos que los de S3 directamente, especialmente a gran escala.
  - **Solicitudes:** CloudFront tiene un costo por solicitud (HTTP/HTTPS).
  - **Nivel Gratuito:** AWS ofrece un nivel gratuito generoso para CloudFront que incluye 1 TB de transferencia de datos y 10 millones de solicitudes HTTP/S al mes, de forma permanente.

Conclusión sobre Costos:

Para la mayoría de los casos de uso de sitios web, usar CloudFront no solo es más seguro, sino que a menudo puede ser más económico que servir el contenido directamente desde S3, gracias al nivel gratuito y a las tarifas de transferencia de datos más bajas.

Cómo Solucionarlo: La Mejor Práctica con CloudFront

La solución recomendada es dejar de exponer el bucket directamente y servir el contenido a través de una distribución de Amazon CloudFront.

1. **Crear una Distribución de CloudFront:**
   - Navega a la consola de **CloudFront** y crea una nueva distribución.
   - Como **origen**, selecciona el bucket de S3 correspondiente.
   - En la sección **Acceso al origen (Origin access)**, selecciona **Origin access control settings (recommended)**. Haz clic en **Crear configuración de control** para generar un nuevo control de acceso. Esto asegura que solo CloudFront pueda acceder al contenido del bucket.
   - CloudFront te proporcionará una **política de bucket** que deberás copiar.
2. **Actualizar la Política del Bucket de S3:**
   - Navega a la consola de **S3** y selecciona el bucket.
   - Ve a la pestaña **Permisos** y edita la **Política del bucket**.
   - **Elimina la declaración (`Statement`) existente** que permite el acceso público (`"Principal": "*"`).
   - **Pega la nueva política** proporcionada por CloudFront. Esta política solo permitirá la acción `s3:GetObject` al principal del servicio de CloudFront.
   - Guarda la política.
3. **Habilitar el Bloqueo de Acceso Público:**
   - En la misma pestaña de **Permisos**, asegúrate de que el **Bloqueo de Acceso Público** esté activado para el bucket. Esto anulará cualquier otra configuración que pudiera permitir el acceso público.
4. **Actualizar DNS/Aplicación:**
   - Una vez que la distribución de CloudFront esté desplegada, actualiza tu aplicación o tus registros DNS para que apunten al nuevo nombre de dominio de CloudFront (ej. `d12345.cloudfront.net`) en lugar de la URL del bucket de S3.

Recomendación

Se recomienda que se dejen de utilizar políticas de bucket públicas y se migre a una arquitectura con **Amazon CloudFront** para servir el contenido de los buckets `banco-`

`imagen-gs-frontend` y `biometricos-frontend`. Este enfoque no solo soluciona el hallazgo de seguridad al restringir el acceso directo, sino que también proporciona beneficios de rendimiento a través de la caché global de CloudFront y a menudo resulta en un ahorro de costos.

Referencias

Examples of Amazon S3 bucket policies - Amazon Simple Storage Service