[Publish] - 7. Exigir el cifrado con Llaves Gestionadas por el Cliente (CMK) para las variables de entorno de Lambda

El hallazgo de seguridad **"Exigir el cifrado con Llaves Gestionadas por el Cliente (CMK) para las variables de entorno de Lambda"** se enfoca en proteger la información sensible que a menudo se almacena en la configuración de una función, como contraseñas, tokens de API o cadenas de conexión a bases de datos.

Por defecto, AWS Lambda cifra estas variables en reposo utilizando una llave gestionada por AWS. Si bien esto ofrece una capa de protección, el uso de una **Llave Gestionada por el Cliente (CMK)** de KMS te proporciona un control de seguridad superior:

- **Separación de Deberes:** Permite que un equipo de seguridad gestione las llaves de cifrado (quién puede usarlas y cómo), mientras que el equipo de desarrollo gestiona el código de la función.
- **Control de Acceso Granular:** Puedes definir políticas de IAM en la CMK para especificar exactamente qué roles o usuarios pueden acceder a las variables de entorno cifradas.
- **Auditoría Centralizada:** Cada vez que Lambda descifra las variables de entorno para una ejecución, esa acción se registra en CloudTrail bajo tu CMK, proporcionando una pista de auditoría clara y centralizada.

Esta práctica es esencial cuando se almacenan datos sensibles directamente en las variables de entorno y es un requisito común en entornos con alta seguridad.

Análisis de las Funciones Lambda Reportadas

Las siguientes funciones Lambda han sido identificadas por no utilizar una Llave Gestionada por el Cliente (CMK) para el cifrado de sus variables de entorno.

Tipo	Nombre de la Función	Número de Cuenta
Lambda	dev-gruposanchezagent2025pocgenia-AthenaQuery	174771279728
Lambda	dev-gruposanchezagent2025pocgenia-FeedbackLambda	174771279728

Lambda	dev-gruposanchezagent2025pocgenia-InvokeAgentLambda	174771279728

Preguntas para tu Equipo (Acción Requerida)

Para remediar este hallazgo, debemos coordinar con el equipo de desarrollo.

1. **¿Contienen estas funciones variables de entorno con información sensible?** Si las variables no contienen secretos (ej. solo nombres de tablas o configuraciones no críticas), el riesgo es menor, aunque la mejor práctica sigue siendo usar una CMK.
2. **¿Existe ya una CMK apropiada en KMS para esta aplicación o entorno?** Si no, será necesario crear una nueva llave.
3. **Permisos del Rol de Ejecución:** ¿El rol de ejecución de IAM asociado a cada función Lambda tiene los permisos necesarios (`kms:Decrypt`) sobre la CMK que se va a utilizar? Si no, la función fallará al intentar leer sus propias variables de entorno.

Consideraciones de Costo

Cambiar de una llave gestionada por AWS a una CMK para el cifrado de variables de entorno introduce un nuevo costo.

- **Llaves Gestionadas por AWS:** El uso de estas llaves es **gratuito**.
- **Llaves Gestionadas por el Cliente (CMKs):**
  - **Costo de Almacenamiento de la Llave:** Cada CMK tiene un costo de **$1 USD al mes**.
  - **Costo de Solicitudes a la API:** Se te cobrará por las solicitudes que el servicio de Lambda haga a KMS para descifrar las variables de entorno cada vez que se "descongela" un entorno de ejecución. Este costo es muy bajo, aproximadamente **$0.03 USD por cada 10,000 solicitudes**.

Conclusión sobre Costos:

El costo de usar una CMK es mínimo (poco más de $1 USD al mes por llave más un pequeño costo variable), pero compra un nivel significativamente más alto de control, seguridad y auditabilidad sobre los secretos almacenados en la configuración de tus funciones.

Cómo Solucionarlo: Configurar el Cifrado con CMK

El proceso para actualizar la configuración de cifrado de una función Lambda es sencillo y no requiere tiempo de inactividad.

1. **Crear/Identificar la CMK:**
   - Navega a la consola de **Key Management Service (KMS)**.
   - Si no tienes una llave adecuada, crea una nueva llave simétrica. Asegúrate de que su política de llave permita al rol de ejecución de la función Lambda realizar la acción `kms:Decrypt`.
2. **Actualizar la Configuración de la Función Lambda:**
   - Navega a la consola de **Lambda** y selecciona la función que deseas modificar.
   - Ve a la pestaña **Configuración** y luego a la sección **Variables de entorno**.
   - Haz clic en **Editar**.
3. **Configurar la Llave de Cifrado:**
   - Desplázate hacia abajo hasta la sección **Cifrado en reposo (Encryption in rest)**.
   - Expande la sección **Configuración de cifrado (Encryption configuration)**.
   - Selecciona **Usar una clave gestionada por el cliente (Use a customer managed key)**.
   - En el menú desplegable, elige la CMK que preparaste en el paso 1.
   - Haz clic en **Guardar**.
4. **Verificar Permisos:**
   - Asegúrate de que el rol de ejecución de la Lambda tenga una política de IAM que le permita usar la llave. Ejemplo de política mínima:

```
{
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:region:ACCOUNT_ID:key/KEY_ID"
}


```

5. **Repetir:** Realiza este proceso para todas las funciones Lambda identificadas.

Recomendación

Se recomienda que se configuren todas las funciones Lambda que manejan información sensible en sus variables de entorno para que utilicen una Llave Gestionada por el Cliente (CMK). Esta es una mejor práctica de seguridad que proporciona un control granular y una auditoría robusta sobre el acceso a los secretos de configuración.

Referencias

Securing Lambda environment variables - AWS Lambda