[Publish] - 3. Los secretos de Secrets Manager deben tener habilitada la rotación automática

El hallazgo de seguridad **"Los secretos de Secrets Manager deben tener habilitada la rotación automática"** resalta una práctica de seguridad crítica para proteger tu entorno en la nube. Almacenar credenciales como contraseñas de bases de datos, llaves de API y claves de cuentas de servicio en AWS Secrets Manager es un excelente primer paso. Sin embargo, los secretos estáticos y de larga duración siguen representando un riesgo. Si un secreto se ve comprometido, puede proporcionar a un atacante acceso prolongado a tus sistemas.

La **rotación automática de secretos** mitiga este riesgo cambiando las credenciales de forma regular y automática. Esta práctica reduce significativamente la vida útil de un secreto comprometido, limitando el daño potencial que un atacante puede causar. Este documento proporciona un análisis de tus secretos actuales y un plan para implementar la rotación automática donde sea apropiado.

Análisis de los Secretos Reportados

Los siguientes secretos han sido identificados por no tener habilitada la rotación automática. Basado en sus nombres, los he agrupado para evaluar mejor la viabilidad y los requisitos para habilitar la rotación.

Tipo	Nombre del Secreto	Número de Cuenta	Propósito Inferido y Tipo de Rotación
SecretsManager	`appflow/498798756906-gs-dlk-appflow-[...]`	498798756906	Múltiples secretos para conexiones de AWS AppFlow (ej. a SAP). Algunos conectores de AppFlow soportan rotación.
SecretsManager	`GitHubAmplifyTokenGr`	174771279728	Token de acceso personal de

	`upoSanchez-mAcMUW`		GitHub para AWS Amplify. Requiere una función Lambda de rotación personalizada.
SecretsManager	`gs-dlk-dev-gs-rds-4iFjg3`	498798756906	Credenciales para una base de datos RDS en un entorno de desarrollo. Utiliza una plantilla de rotación gestionada por AWS.
SecretsManager	`prod/biometricos-4EPrgn`	002670977573	Secreto de producción para la aplicación "biometricos". El tipo es desconocido y requiere investigación.

Lista completa:

Tipo	**Nombre**	**Número de cuenta**
SecretsManager	appflow!498798756906-gs-dlk-appflow-ADRC-prueba-1742594389358-q5Mq1I	498798756906
SecretsManager	appflow!498798756906-gs-dlk-appflow-test-1740762107414-4GQ20v	498798756906
SecretsManager	appflow!498798756906-gs-dlk-appflow-test-	498798756906

	1740764696031-aLJxO9	
SecretsManager	appflow!498798756906-new_conection-1749159848730-B2c2NJ	498798756906
SecretsManager	appflow!498798756906-sap-connect-test-1740761691262-jBdRGQ	498798756906
SecretsManager	appflow!498798756906-sap-connect-test-1741870452327-rxEUAU	498798756906
SecretsManager	appflow!498798756906-sap-connect-test-ADCR-1742594580589-smoj5X	498798756906
SecretsManager	GitHubAmplifyTokenGrupoSanchez-mACmUW	174771279728
SecretsManager	gs-dlk-dlk-dev-gs-rds-4iFJg3	498798756906
SecretsManager	prod/biometricos-4EPrgn	002670977573

Preguntas para tu Equipo (Acción Requerida)

Habilitar la rotación no es un proceso único para todos. El método depende del tipo de secreto y de los servicios que lo utilizan. Para avanzar, por favor discute las siguientes preguntas con tus equipos de aplicación e infraestructura para cada categoría de secreto.

- **Para los secretos de AppFlow:** ¿A qué servicios específicos se conectan estos flujos (ej. SAP, Salesforce)? Se necesita verificar si el conector de AppFlow correspondiente soporta la rotación de credenciales.
- **Para el token de GitHub:** ¿Las aplicaciones que usan este token están preparadas para obtener la nueva versión del secreto después de una rotación? Será necesario desarrollar una función Lambda personalizada que utilice la API de GitHub para rotar el token.
- **Para el secreto de RDS (`gs-dlk-dev-gs-rds`):** ¿Se puede programar una breve ventana para habilitar la rotación? AWS puede gestionar esto de forma nativa, pero es bueno validar que la aplicación recupere la nueva contraseña sin problemas después de la primera rotación.

- **Para el secreto `prod/biometricos`:** ¿Qué tipo de credencial es esta? ¿Es una contraseña de base de datos, una llave de API de un tercero o algo más? Conocer el tipo es el primer paso para determinar cómo se puede rotar.

Consideraciones de Costo

Habilitar la rotación automática introduce costos nuevos, aunque generalmente mínimos, de los servicios subyacentes que facilitan el proceso.

- **AWS Secrets Manager:**
  - **Almacenamiento del Secreto: $0.40 USD por secreto al mes.** Este costo es el mismo, con o sin rotación.
  - **Llamadas a la API: $0.05 USD por cada 10,000 llamadas.** La rotación aumentará ligeramente el número de llamadas a la API.
- **AWS Lambda (Usado para la Rotación):**
  - **Costo de Ejecución:** Se factura por el número de solicitudes y la duración.
  - **Nivel Gratuito:** El generoso nivel gratuito permanente de Lambda (1 millón de solicitudes/mes) probablemente cubrirá todos los costos de rotación para un número moderado de secretos.
- **AWS Key Management Service (KMS):**
  - **Llamadas a la API:** La función Lambda de rotación debe hacer llamadas a KMS para descifrar el secreto, lo que genera un costo muy pequeño (**$0.03 USD por 10,000 solicitudes**).

Conclusión sobre Costos:

Sí, habilitar la rotación genera más costos, principalmente por un pequeño aumento en las llamadas a la API de KMS y Secrets Manager. Sin embargo, para la mayoría de los casos, este aumento es insignificante (centavos por secreto). Los enormes beneficios de seguridad de eliminar credenciales estáticas superan con creces este costo mínimo.

Cómo Solucionarlo: Habilitar la Rotación

Una vez que tengas las respuestas a las preguntas anteriores, el proceso general es el siguiente:

1. **Identificar la Estrategia de Rotación:** Determina si puedes usar una plantilla de rotación gestionada por AWS (como para RDS) o si necesitas una función Lambda personalizada (como para el token de GitHub).
2. **Configurar la Función Lambda:**

- **Para rotación gestionada por AWS:** Despliega la aplicación preconstruida apropiada desde el AWS Serverless Application Repository (SAR).
- **Para rotación personalizada:** Desarrolla una función Lambda que contenga la lógica para crear una nueva versión del secreto, actualizar la credencial en el servicio final (ej. en la API de GitHub) y marcar la nueva versión como la actual.

3. **Configurar la Rotación en Secrets Manager:** En la configuración del secreto, habilita la rotación automática, apunta a la función Lambda que configuraste y establece un calendario (ej. cada 30, 60 o 90 días).
4. **Probar y Verificar:** Después de la primera rotación, prueba a fondo las aplicaciones que dependen del secreto para asegurarte de que hayan recuperado la nueva credencial y funcionen correctamente.

Recomendación

Se recomienda que se inicie un plan para habilitar la rotación automática en todos los secretos listados, priorizando los de producción (`prod/biometricos`) y los que otorgan acceso a sistemas críticos como RDS. La rotación de secretos es una de las defensas más efectivas contra el uso indebido de credenciales a largo plazo.

Referencias

Rotate AWS Secrets Manager secrets - AWS Secrets Manager