Nueva investigación en ciberseguridad ha descubierto que las herramientas de interfaz de línea de comandos (CLI) de Amazon Web Services (AWS) y Google Cloud pueden exponer credenciales confidenciales en registros de compilación, lo cual representa riesgos considerables para las empresas.

Esta vulnerabilidad ha sido etiquetada como LeakyCLI por la firma de seguridad en la nube Orca.

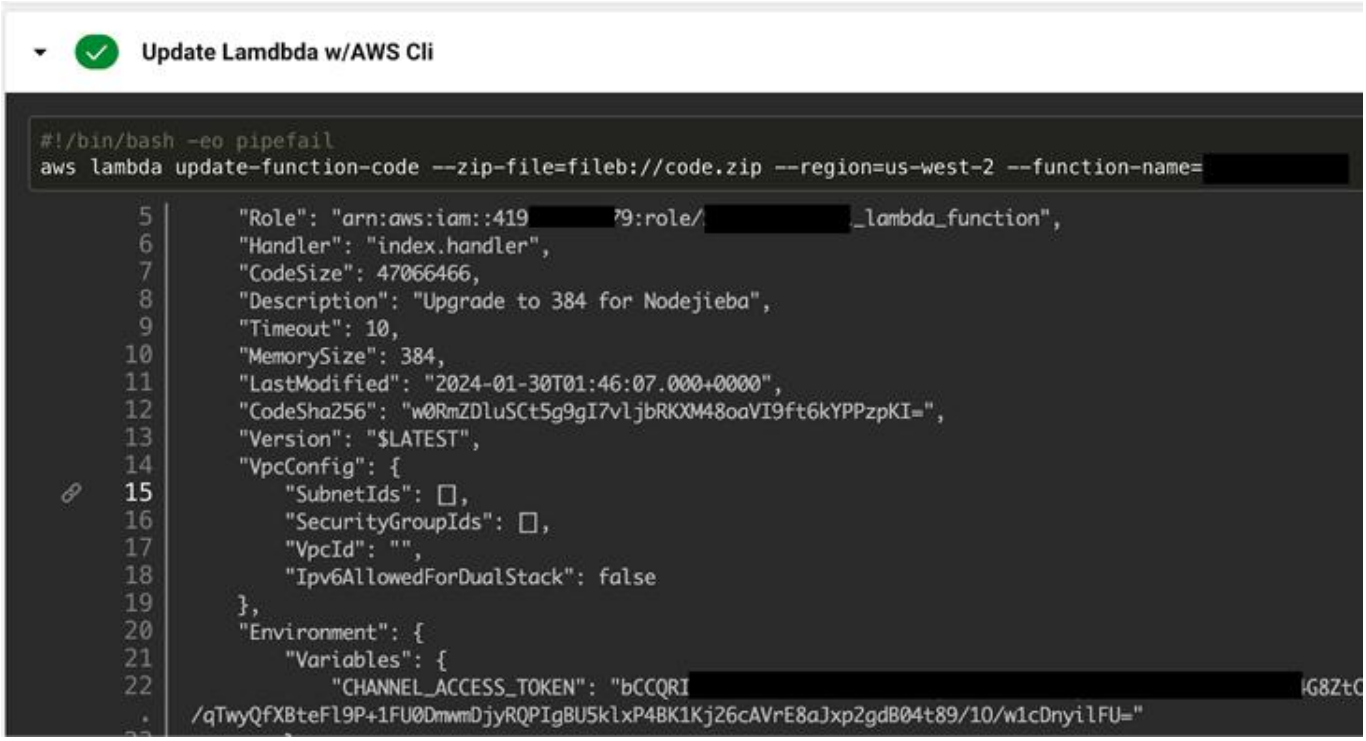
> *«Algunos comandos en Azure CLI, AWS CLI y Google Cloud CLI pueden revelar información sensible en forma de variables de entorno, que pueden ser aprovechadas por atacantes cuando son publicadas por herramientas como GitHub Actions»,* explicó el investigador de seguridad Roi Nisimi en un informe.

Microsoft ha abordado este problema como parte de las actualizaciones de seguridad lanzadas en noviembre de 2023, asignándole el identificador CVE CVE-2023-36052 (puntuación CVSS: 8.6).

En resumen, la idea radica en cómo los comandos de CLI, como los mencionados anteriormente, pueden utilizarse para mostrar variables de entorno predefinidas y generar registros en los procesos de Integración Continua y Despliegue Continuo (CI/CD). A continuación se presenta una lista de tales comandos que abarcan tanto AWS como Google Cloud:

- aws lambda get-function-configuration
- aws lambda get-function
- aws lambda update-function-configuration
- aws lambda update-function-code
- aws lambda publish-version
- gcloud functions deploy –set-env-vars
- gcloud functions deploy –update-env-vars
- gcloud functions deploy –remove-env-vars

Orca informó haber encontrado varios proyectos en GitHub que, sin darse cuenta, filtraron tokens de acceso y otros datos sensibles a través de los registros de GitHub Actions, CircleCI, TravisCI y Cloud Build.



A diferencia de Microsoft, tanto Amazon como Google consideran que este comportamiento es esperado, y requieren que las organizaciones tomen medidas para evitar almacenar secretos en variables de entorno, optando en su lugar por utilizar un servicio de almacenamiento de secretos dedicado, como AWS Secrets Manager o Google Cloud Secret Manager.

Google también sugiere utilizar la opción *«–no-user-output-enabled»* para suprimir la impresión de la salida del comando en la salida estándar y en el error estándar en la terminal.

> *«Si los ciberdelincuentes obtienen acceso a estas variables de entorno, podrían potencialmente acceder a información confidencial, como contraseñas, nombres de usuario y claves, lo que les permitiría acceder a cualquier recurso que los propietarios del repositorio puedan tener»*, advirtió Nisimi.
>
> *«Los comandos de CLI se consideran por defecto que se ejecutan en un entorno seguro, pero en combinación con los pipelines de CI/CD, pueden representar una amenaza para la seguridad.»*