Investigadores de ciberseguridad han revelado una vulnerabilidad que afecta al Kit de Desarrollo de la Nube (CDK) de Amazon Web Services (AWS), la cual podría haber permitido la toma de control de una cuenta en condiciones específicas.

> *«El impacto de este fallo podría, en ciertos casos, permitir que un atacante obtenga acceso administrativo a una cuenta de AWS, resultando en la toma total de control de la cuenta»*, indicó Aqua en un informe.

Tras una divulgación responsable el 27 de junio de 2024, los mantenedores del proyecto solucionaron el problema en la versión 2.149.0 del CDK, lanzada en julio.

El AWS CDK es un marco de desarrollo de software de código abierto que permite definir recursos para aplicaciones en la nube utilizando lenguajes como Python, TypeScript o JavaScript, y aprovisionarlos mediante CloudFormation.

El fallo descubierto por Aqua se basa en investigaciones anteriores de la firma de seguridad en la nube sobre recursos ocultos en AWS, y cómo los nombres predefinidos para los buckets de AWS Simple Storage Service (S3) podrían explotarse para llevar a cabo ataques de *«Monopolio de Bucket»* y obtener acceso a datos sensibles.

El proceso de preparación de un entorno de AWS para su uso con el CDK se denomina «bootstrap» y consiste en aprovisionar ciertos recursos de AWS en el entorno, como un bucket S3, un repositorio de Amazon Elastic Container Registry (ECR), y roles de AWS Identity and Access Management (IAM).

> *«Los recursos y su configuración utilizados por el CDK están definidos en una plantilla de AWS CloudFormation»,* según la documentación de AWS.
>
> *«Para iniciar un entorno, se usa el comando cdk bootstrap de la Interfaz de Línea de*

> *Comandos de AWS CDK (CLI). Esta CLI recupera la plantilla y la despliega en AWS CloudFormation como una pila llamada 'bootstrap stack'. Por defecto, esta pila se nombra CDKToolkit».*

Algunos de los roles de IAM creados durante el proceso de bootstrapping otorgan permisos para cargar y eliminar activos del bucket S3 correspondiente, así como realizar implementaciones de pilas con acceso administrativo.

Aqua destacó que los nombres de los roles de IAM creados por el CDK de AWS siguen el formato *«cdk-{Calificador}-{Descripción}-{ID-de-Cuenta}-{Región}»*, donde cada campo se describe a continuación:

- Calificador: una cadena única de nueve caracteres que por defecto es «hnb659fds», aunque puede personalizarse durante la fase de bootstrapping.
- Descripción: una descripción del recurso (por ejemplo, cfn-exec-role).
- ID-de-Cuenta: el ID de la cuenta de AWS del entorno.
- Región: la región de AWS del entorno.

De manera similar, el bucket S3 creado durante el bootstrapping sigue el patrón de nombre *«cdk-{Calificador}-assets-{ID-de-Cuenta}-{Región}».*

> *«Dado que muchos usuarios ejecutan el comando cdk bootstrap sin modificar el calificador, el patrón de nombres del bucket se vuelve predecible. Esto es porque el valor por defecto del calificador es 'hnb659fds', lo que hace que sea más fácil adivinar el nombre del bucket»,* dijo Aqua.

Con miles de ejemplos descubiertos en GitHub donde se usa el calificador predeterminado, esto implica que adivinar el nombre del bucket es tan sencillo como encontrar el ID de la cuenta de AWS y la región donde se despliega el CDK.

Al combinar este aspecto con el hecho de que los nombres de los buckets S3 son únicos a nivel global en todas las cuentas de AWS, se abre la posibilidad de realizar un ataque conocido como «S3 Bucket Namesquatting» (o «Bucket Sniping»), en el que un atacante puede reclamar el bucket del CDK de otro usuario si aún no existe.

Esto podría causar una denegación de servicio (DoS) parcial cuando el usuario intenta realizar el bootstrap del CDK con el mismo ID de cuenta y región. Esta situación podría evitarse al especificar un calificador personalizado durante el proceso.

Un escenario más grave podría presentarse si el CDK de la víctima tiene permisos para leer y escribir datos en un bucket S3 controlado por el atacante, lo que permitiría modificar las plantillas de CloudFormation y ejecutar acciones maliciosas dentro de la cuenta de AWS de la víctima.

> *«El rol de despliegue del servicio de CloudFormation, conocido como CloudFormationExecutionRole en CDK, tiene privilegios administrativos en la cuenta por defecto»,* explicó Aqua.
>
> *«Esto significa que cualquier plantilla de CloudFormation escrita en el bucket S3 del atacante por el CDK de la víctima se implementaría posteriormente con privilegios administrativos en la cuenta de la víctima, lo que permitiría al atacante crear recursos con privilegios elevados».*

En un ataque hipotético, si un usuario hubiera iniciado el proceso de bootstrap del CDK en el pasado y luego eliminara el bucket S3 debido a los límites de cuota, un atacante podría aprovechar esta situación para crear un bucket con el mismo nombre.

Esto haría que el CDK confíe implícitamente en el bucket malicioso y lea/escriba plantillas de CloudFormation en él, dejándolas vulnerables a la explotación. No obstante, para que este ataque tenga éxito, el atacante debería cumplir con los siguientes requisitos:

- Reclamar el bucket con el nombre predecible y permitir acceso público.
- Crear una función Lambda que inyecte un rol administrativo malicioso o una puerta trasera en cualquier plantilla de CloudFormation cuando se suba al bucket.

En la última etapa, cuando el usuario despliega el CDK usando «cdk deploy», no solo se envía la plantilla al bucket réplica, sino que también se inyecta un rol administrativo que el atacante podría asumir, logrando así el control total de la cuenta de la víctima.

En resumen, la cadena de ataque permite crear un rol de administrador en una cuenta de AWS objetivo cuando se elimina un bucket de S3 creado por CDK durante el proceso de inicialización, y luego se vuelve a usar CDK. AWS ha confirmado que cerca del 1% de los usuarios de CDK fueron vulnerables a este vector de ataque.

La corrección implementada por AWS asegura que los activos solo se suban a los buckets dentro de la cuenta del usuario, evitando que CDK envíe datos a buckets que no pertenezcan a la cuenta que inició el proceso de inicialización. AWS también recomendó a los usuarios emplear un calificador personalizado en lugar del valor predeterminado «hnb659fds».

En una declaración a *The Hacker News*, AWS afirmó que investigó y resolvió todas las preocupaciones relacionadas con la exposición no autorizada de datos durante las implementaciones de CDK.

> *«El 12 de julio de 2024, AWS lanzó una actualización del AWS Cloud Development Kit (AWS CDK) CLI que agregó controles de seguridad adicionales para reducir el riesgo de divulgación de datos para los clientes que realizan implementaciones de CDK»*, comentó un portavoz de AWS.
>
> *«Los usuarios de la versión más reciente necesitarán realizar una acción única para actualizar los recursos de inicialización. AWS ha contactado directamente a los clientes potencialmente afectados para notificarles sobre la necesidad de actualización, y ha añadido verificaciones adicionales al CLI para recordarles a los*

> *usuarios que deben realizar la actualización.»*

Dicho esto, los usuarios que hayan realizado la inicialización con una versión v2.148.1 o anterior de CDK tendrán que actualizar a la versión más reciente y ejecutar nuevamente el comando de inicialización. Como alternativa, pueden aplicar una condición de política IAM al rol *FilePublishingRole* de CDK.

Estos hallazgos subrayan la importancia de mantener los ID de las cuentas de AWS en privado, definir políticas IAM con un alcance limitado, y evitar nombres predecibles para los buckets de S3.

> *«En su lugar, generen identificadores únicos o hashes aleatorios por región y cuenta, e incorporen estos en los nombres de los buckets de S3. Esta estrategia ayuda a prevenir que los atacantes reclamen su bucket de forma anticipada»,* recomendó Aqua.

Este descubrimiento se produce al mismo tiempo que Symantec, propiedad de Broadcom, identificó varias aplicaciones de Android e iOS que incluían credenciales de servicios en la nube de AWS y Microsoft Azure Blob Storage incrustadas y sin cifrar, lo que pone en riesgo los datos de los usuarios.

Algunas de las aplicaciones implicadas incluyen *Pic Stitch: Collage Maker*, *Crumbl*, *Eureka: Earn Money for Surveys*, *Videoshop – Video Editor*, *Meru Cabs*, *Sulekha Business* y *ReSound Tinnitus Relief*.

> *«Esta práctica peligrosa implica que cualquier persona con acceso al binario o al código fuente de la aplicación podría extraer estas credenciales y usarlas indebidamente para manipular o extraer datos, lo que podría resultar en graves brechas de seguridad»*, explicaron los investigadores de seguridad, Yuanjing Guo y

> Tommy Dong.