I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Sistemas y/o software abierto

Nivel de riesgo: Media

II. ALERTA

Ciber atacantes estarían explotando vulnerabilidades existentes en MinIO, y consecuentemente accediendo de manera no autorizada a información privada, ejecución de código malicioso y tomar control total de servidores para la ejecución de otras actividades de ataque.

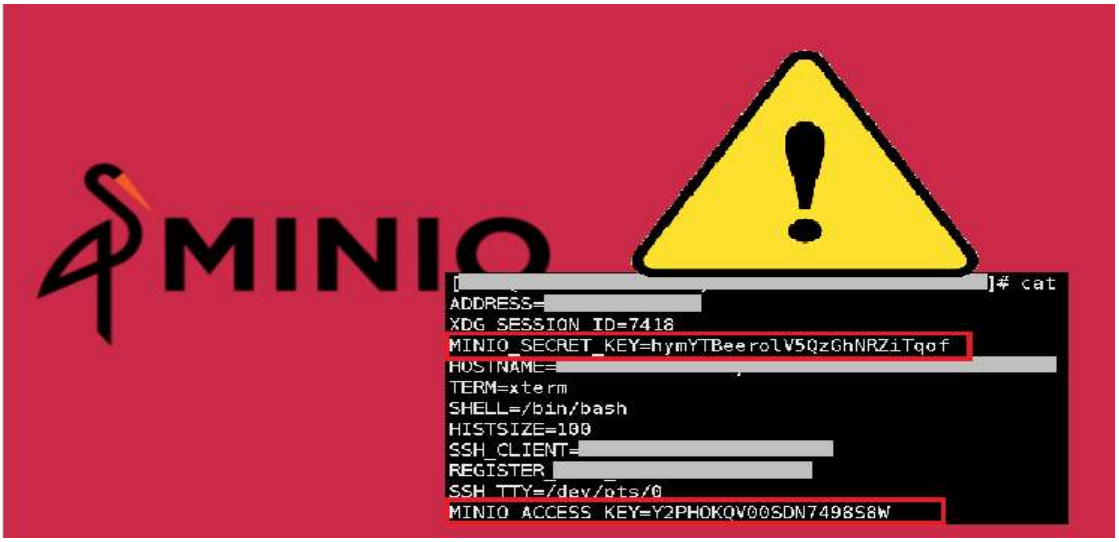

Figura 1.- lustración relacionada a vulnerabilidades MinIO
Fuente: Elaboración Propia

III. INTRODUCCIÓN

MinIO es un sistema de almacenamiento por objetos que se encuentra a disposición de la comunidad bajo licencia de tipo AGPLv3. Debido a la compatibilidad con el API S3 de Amazon, capacidad de ser utilizable en una variedad de implementaciones y la interacción con otras aplicaciones de código abierto, MinIO es una gran herramienta para desarrollo y pruebas.

Las pruebas de concepto técnicas indican que en un entorno de tipo cluster, la implantación de ciertas versiones de MinIO, todas las variables de entorno podrían ser accedidas como parámetros de consulta, lo que a su vez implica divulgación de no autorizada de información. Las variables que representan mayor riesgo al ser expuestas son MINIO_SECRET:KEY y MINIO:ROOT_PASSWORD.

Las versiones MinIO que presentan vulnerabilidades se encuentran entre el rango comprendido entre RELEASE.2019-12-17T23-16-33Z y las anteriores a RELEASE.2023-03-20T20-16-18Z. Las características técnicas específicas de la explotación de las vulnerabilidades detectadas, se encuentran registradas en el formulario de priorización de riesgos CVE, CVE-2023-28432 y CVE-2023-28434

IV. VECTOR DE ATAQUE:

- Ataques de ingeniería social
- Conexiones remotas desde la red de Internet

V. IMPACTO:

- Instalación no autorizada de aplicaciones.
- Acceso no autorizado a información sensible.
- Acceso no autorizado para creación, lectura, modificación y eliminación de activos de información.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Aplicar las actualizaciones de seguridad de acuerdo a las instrucciones del desarrollar.
- Aislar secciones críticas de red en consideración a la criticidad y sensibilidad de los activos de información vinculados a los dispositivos de seguridad vulnerables.
- Aplicar el principio de menor privilegio en la creación de perfiles de usuario.
- Utilizar múltiples factores de autenticación.

VII. REFERENCIAS:

- MINIO. Understanding the Attack Vector for CVE-2023-28432 and CVE-2023-28434. (08 de 09 de 2023). Obtenido de https://blog.min.io/security-advisory-stackedcves/
- NIST. CVE-2023-28432. (28 de 03 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2023-28432
- NIST. CVE-2023-28434. (28 de 03 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2023-28434
- JOES. New Attack Vector In The Cloud: Attackers caught exploiting Object Storage Services. (04 de 09 de 2023). Obtenido de https://www.securityjoes.com/post/new-attack-vector-in-the-cloud-attackers-caught-exploiting-object-storage-services?ref=blog.min.io