Un actor no identificado ha sido detectado utilizando vulnerabilidades críticas en el sistema de almacenamiento de objetos de alto rendimiento MinIO para lograr la ejecución no autorizada de código en servidores afectados.

La empresa de ciberseguridad y respuesta a incidentes Security Joes informó que la intrusión se llevó a cabo mediante una cadena de exploits de acceso público para instalar una puerta trasera en la instancia de MinIO.

Las vulnerabilidades en cuestión son CVE-2023-28432 (con una calificación CVSS de 7.5) y CVE-2023-28434 (con una calificación CVSS de 8.8), siendo la primera de ellas añadida al catálogo de Vulnerabilidades Conocidas Explotadas (KEV) de la Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) el 21 de abril de 2023.

De acuerdo con un informe por parte de Security Joes, estas dos vulnerabilidades *«tienen el potencial de exponer información sensible presente en la instalación comprometida y permitir la ejecución remota de código (RCE) en el host donde se encuentra operativa la aplicación MinIO».*

En el proceso de ataque investigado por la compañía, se informa que las vulnerabilidades fueron utilizadas por el atacante para obtener credenciales de administrador y aprovechar esa posición para sustituir el cliente MinIO en el host por una versión alterada, activando un comando de actualización que especifica una MIRROR_URL.

> *«El comando de actualización 'mc admin update' actualiza todos los servidores MinIO en la implementación. Este comando también admite el uso de un servidor espejo privado para entornos en los que la implementación no tenga acceso a Internet público»,* según se detalla en la documentación de MinIO.

> Security Joes explicó: *«El resultado de estas acciones permite que el atacante orqueste una actualización engañosa. Al reemplazar el binario MinIO genuino por su*

> *versión 'maliciosa', el atacante asegura la comprometida del sistema».*

Las modificaciones maliciosas en el binario exponen un punto de entrada que recibe y ejecuta comandos a través de solicitudes HTTP, funcionando efectivamente como una puerta trasera. Los comandos heredan los permisos del sistema del usuario que inició la aplicación.

Es relevante mencionar que la versión alterada del binario es una réplica de un exploit denominado «Evil MinIO» que se publicó en GitHub a principios de abril de 2023. Sin embargo, no existe evidencia que sugiera una conexión entre ambos.

Lo que es evidente es que el actor de amenazas es hábil en el uso de scripts bash y Python, además de aprovechar el acceso a la puerta trasera para cargar componentes adicionales desde un servidor remoto para la post-explotación mediante un script de descarga.

Este script, que puede dirigirse tanto a entornos Windows como Linux, sirve como un punto de entrada para analizar los hosts comprometidos, en función de lo cual se decide si se debe o no poner fin a la ejecución.

Security Joes señaló: *«Este enfoque dinámico resalta la estrategia del actor de amenazas para optimizar sus esfuerzos en función del valor percibido del sistema comprometido».*