



Docker Hub, una de las bibliotecas de imágenes más grandes en la nube, sufrió una violación de datos después de que un atacante desconocido obtuviera acceso a la única base de datos de Hub de la compañía.

Docker Hub es un servicio de repositorio en línea donde los usuarios y socios pueden crear, probar, almacenar y distribuir imágenes de contenedor de Docker, tanto de forma pública como privada.

La brecha expuso información confidencial para casi 190,000 usuarios de Hub (menos del 5% del total de usuarios), incluidos los nombres de usuarios y contraseñas de hash para un pequeño porcentaje de usuarios afectados, así como tokens de GitHub y Bitbucket para los repositorios de Docker.

Docker Hub comenzó a notificar a los usuarios afectados mediante correos electrónicos informándoles sobre el incidente de seguridad y pidiéndoles que cambien sus contraseñas para Docker Hub, así como cualquier cuenta en línea que use la misma contraseña.

*«El jueves 25 de abril de 2019, descubrimos un acceso no autorizado a una única base de datos Hub que almacena un subconjunto de datos de usuarios no financieros. Al descubrirlo, actuamos rápidamente para intervenir y asegurar el sitio».*

*«Para los usuarios con autobuilds que pueden haber sido afectados, hemos revocado tokens y claves de acceso de GitHub, y le pedimos que vuelva a conectarse a sus repositorios y verifique los registros de seguridad para ver si se han producido acciones inesperadas».*

La compañía no ha revelado más detalles acerca del incidente de seguridad o sobre cómo los atacantes desconocidos obtuvieron acceso a su base de datos.



Docker afirma que la compañía sigue investigando la brecha de seguridad y compartirá más información cuando esté disponible.

La compañía también trabaja para mejorar sus procesos de seguridad generales y revisar sus políticas después de la violación.