Docker Hub - User Notification

1 message

Docker Hub Team <goto@docker.com>   Fri, Apr 26, 2019 at 9:57 PM
Reply-To: info@docker.com
To:████████████████

docker

On Thursday, April 25th, 2019, we discovered unauthorized access to a single Hub database storing a subset of non-financial user data. Upon discovery, we acted quickly to intervene and secure the site.

We want to update you on what we've learned from our ongoing investigation, including which Hub accounts are impacted, and what actions users should take.

Here is what we've learned:

During a brief period of unauthorized access to a Docker Hub database, sensitive data from approximately 190,000 accounts may have been exposed (less than 5% of Hub users). Data includes usernames and hashed passwords for a small percentage of these users, as well as Github and Bitbucket tokens for Docker autobuilds.

Actions to Take:

- We are asking users to change their password on Docker Hub and any other accounts that shared this password.
- For users with autobuilds that may have been impacted, we have revoked GitHub tokens and access keys, and ask that you reconnect to your repositories and check security logs to see if any unexpected actions have taken place.
  - You may view security actions on your GitHub or BitBucket accounts to see if any unexpected access has occurred over the past 24 hours -see https://help.github.com/en/articles/reviewing-your-security-log and

https://bitbucket.org/blog/new-audit-logs-give-you-the-who-what-when-and-where

- This may affect your ongoing builds from our Automated build service. You may need to unlink and then relink your Github and Bitbucket source provider as described in https://docs.docker.com/docker-hub/builds/link-source/

We are enhancing our overall security processes and reviewing our policies. Additional monitoring tools are now in place.

Our investigation is still ongoing, and we will share more information as it becomes available.

Thank you,

Kent

Kent Lamb
Director of Docker Support
info@docker.com