Issue

On Thursday, April 25th, 2019, we discovered unauthorized access to a single Docker 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.

Resolution

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.

- 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. This means your autobuilds will fail, and we 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 verify if any unexpected access has occurred - see https://help.github.com/en/articles/reviewing-your-security-log (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 (https://bitbucket.org/blog/new-audit-logs-give-you-the-who-what-when-and-where)
    - 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/ (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.

Frequently Asked Questions

Q: What happened?

There was a brief period of unauthorized access to a Docker Hub database. During this time some 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 users as well as GitHub and Bitbucket tokens for Docker autobuilds. All these tokens have been revoked.

Q: Were any of the Docker Official Images impacted by this incident?

No Official Images have been compromised. We have additional security measures in place for our Official Images including GPG signatures on git commits as well as Notary signing to ensure the integrity of each image.

Q: How do I know if I was impacted by this unauthorized access?

If you directly received an email from Docker about this incident, you may have been impacted. If you have received a password reset link, your password hash was potentially exposed. We have invalidated it and sent you a password reset link as a precaution. If you are using autobuilds and your GitHub or Bitbucket repositories have been unlinked from Docker Hub, you will need to relink those repositories for autobuilds to work correctly.

Q: What do I need to do?

For all Docker Hub users, there is no action required to preserve your security. A password reset link has been sent to any users who potentially had their password hash exposed. Users who have autobuilds who have had their GitHub or Bitbucket repositories unlinked will need to relink those repositories.

Q: Do I need to reset my password on Docker Hub?

No. If your password hash was potentially exposed, we have invalidated your password and emailed you a reset password link. Even if you did not receive a password reset link, it's never a bad idea to change your password (https://id.docker.com/reset-password/?service=43f17c5f-9ba4-4f13-853d-9d0074e349a7) if you haven't changed it in a while.

Q: Why did you delete my GitHub tokens before notifying me?

Revoking the tokens was done as soon as possible to protect users. At that point in time we were working on additional measures to secure the site. Once completed, communications were sent to all potentially impacted users.

Q: If I relink my Docker Hub repository to a GitHub repository will I be at risk?

No. Relinking your Docker Hub repository will create a new read-only deploy key to your GitHub or Bitbucket source repositories.

Q: I can't sign in to Docker Hub, have I been hacked?

We have sent a password reset link to each user whose password hash may have been impacted. Please check your email to see if you have received a password reset link. If you have any concerns, please contact info@docker.com.

Q: I have never used the Docker Hub Autobuild feature. Why did I receive an email?

You may have linked your GitHub or Bitbucket account to Docker Hub in the past or your password hash was potentially exposed. If you did link your account to Docker Hub, we have unlinked it. If your password hash was potentially exposed, we have invalidated it and sent you a password reset link as a precaution.