github.blog

GitHub Security Update: Reused password attack - The GitHub Blog

2 minutes

What happened?

On Tuesday evening PST, we became aware of unauthorized attempts to access a large number of GitHub.com accounts. This appears to be the result of an attacker using lists of email addresses and passwords from other online services that have been compromised in the past, and trying them on GitHub accounts. We immediately began investigating, and found that the attacker had been able to log in to a number of GitHub accounts.

GitHub has not been hacked or compromised.

What information was involved?

For affected accounts, usernames and passwords are involved. Additionally, for some accounts, other personal information including listings of accessible repositories and organizations may have been exposed.

What we are doing:

In order to protect your data we've reset passwords on all affected accounts. We are in the process of sending individual notifications to affected users.

What you can do:

If your account was impacted, we are in the process of contacting you directly with information about how to reset your password and restore access to your account.

We encourage all users to practice good password hygiene and enable two-factor authentication to protect your account.

These attacks often evolve, and we're continuing to investigate and monitor for new attack vectors. Please keep an eye on our blog and on Twitter for pertinent updates, or contact Support if you have any questions.