Dropbox Security Bug Made Passwords Optional For Four Hours

Jason Kincaid
@jasonkincaid / 9 years

This morning a post on Pastebin outlined a serious security issue that was spotted at Dropbox: for a brief period of time, the service allowed users to log into accounts using any password. In other words, you could log into someone's account simply by typing in their email address. Given that many people entrust **Dropbox** ⓘ with important data (one of the service's selling points is its security), that's a really big deal.

We've now confirmed with Dropbox that the service did have this issue yesterday — Dropbox says that it began after a code push at 1:54 PM PDT and was fixed at 5:46 PM PDT (they had the fix live five minutes after they discovered it). So, in total, the bug was live for around four hours.

The question now is how many people were affected. The company will be announcing that "much less than 1 percent" of users logged in during this time, and that all sessions have now been logged out as a security precaution. The team is now investigating if any accounts were improperly accessed, and says that anyone who was impacted will be notified.

Update: Here's the company's blog post, which just went live:

> Hi Dropboxers,
>
> Yesterday we made a code update at 1:54pm Pacific time that introduced a bug affecting our authentication mechanism. We discovered this at 5:41pm and a fix was live at 5:46pm. A very small number of users (much less than 1 percent) logged in during that period, some of whom could have logged into an account without the correct password. As a precaution, we ended all logged in sessions.
>
> We're conducting a thorough investigation of related activity to understand whether any accounts were improperly accessed. If we identify any specific instances of unusual activity, we'll immediately notify the account owner. If you're concerned about any activity that has occurred in your account, you can contact us atsecurity@dropbox.com.
>
> This should never have happened. We are scrutinizing our controls and we will be implementing additional safeguards to prevent this from happening again.
>
> -Arash

The issue was posted to Pastebin by Christopher Soghoian, who has previously criticized Dropbox for the company's misleading description of its security practices (Dropbox used to claim that employees at the company had no way of viewing user files, but in reality a small number of them do have administrative privileges). Soghoian didn't discover the password issue himself — it was relayed to him and he anonymized the email exchange.

Security scares are the last thing Dropbox needs. The company has seen very strong growth over the last year and is rumored to have a valuation that may be as high as $1.5 or 2 *billion*. But all of this growth is contingent on people trusting the service — the whole point is that you're mirroring your most important and most frequently-accessed files between multiple computers. If people start worrying that their Excel spreadsheet or banking data or private IMs could be exposed, they'll turn elsewhere.

Most people probably don't care if Dropbox employees could conceivably access their files (after all, the same is true at Google and Facebook). But an authentication system that's accepting the wrong password? That's something that anyone can understand (and get scared about). I love Dropbox and have been using the service for years now, but gaping security holes like this simply aren't acceptable — especially when there are other services that offer similar functionality. Even if nobody accessed my account (which is probably the case), the fact that this *could* happen is unnerving.

Here's one of the email messages posted to Pastebin that describes the issue:

> Hi Chris,
>
> If you're still involved in the dropbox investigation, there was an interesting development this afternoon. I found I was able to log into my account using an incorrect password, and on further investigation I found I could log in and access files on any of the three accounts I tested (mine and two friends') using any password.
>
> This is corroborated by the admittedly-thin dropbox tech support thread below.
>
> So evidently they fail open when auth is busted, or sometimes they roll dev code, or….? This has me really bummed because I just "fixed" my exposure to website password theft by generating gnarly passwords with keypass and storing them on dropbox. Sigh.

And here's a response that, according to the Pastebin post, came from Dropbox CTO Arash Ferdowsi:

> Arash Ferdowsi, Jun-19 06:08 pm (PDT):
>
> hi XXX,
> there was a very brief glitch and this should never happen/be possible again. thanks for the email.