What you need to know about the recent MangaDex data breach (Thread)

Hallo hallo,

Getting directly to the point, a hacker was able to obtain a copy of our code, and as we've recently discovered, a copy of our database which appears to be about four months old. The hacker made his first public appearance two days ago by posting the website code online claiming he acquired a copy of it through a PHP RCE (remote code execution) and attempted to ransom us for "10k BTC [sic] or everything goes public."

After assessing our current code and server infrastructure, we came to the conclusion that they were secure, and that if he managed to get a copy of our code, it had to have been from a server that we no longer used and could no longer check.

When asked for proof about the existence of a database dump, he refused and spammed "HOMBREEEEEE". The lack of willingness to show proof about the db dump to make a more convincing ransom argument led us to believe that while he may have had an outdated copy of the source code, he didn't have a copy of the db. That assumption was incorrect. Despite being an outdated one, they did possess such a copy.

Using their database dump, the hacker was able to use the session codes stored in the db when you hit "remember me" to bypass any password and 2FA requirements, as these are stored for a couple of months.

They then proceeded to log into the account of our admin, and entertained themselves for a bit by deleting a few of the most popular groups and then making a fake announcement. Within a minute of discovering his actions, we were able to take the site and API servers down immediately.

Is the site secure?

While the site clearly has at some point been abused to acquire the source code and database dump, we are continuously monitoring and investigating potential security holes in our infrastructure, and fixing any we identify while doing so.

We have now reached a point where we are confident in our infastructure’s current state, and believe that the methods used to gain undue access in the past couldn’t be used again. Additionally, if he ever had remote access to our servers, he does not anymore.

Finally, we have not seen any conclusive evidence of the accesses being used to distribute harmful content to our users, but will continue monitoring in that regard.

The Database Leak

As of writing this announcement the hacker hasn't dumped the database online yet but it is more or less an inevitability. Your passwords are stored in the database hashed and salted with a secure algorithm (bcrypt), meaning your password cannot be leaked as plaintext. Regardless of this, you should still change your password for MD and never use that password anywhere else. However, email addresses, creation and last connection IPs, backup 2FA codes, RSS keys, follows, comments, DMs, etc. would be spread out in the event that the database dump is made public, which you should assume will be the case.

We've cleared out the sessions table so anyone that was logged in will be logged out (you might need to clear your cookies too). The backup 2FA codes were compromised so we've removed 2FA from all accounts. Personal RSS keys for your manga follows were also compromised, and have been reset. Any existing RSS feeds will need the new key edited in to continue functioning.

Actions we recommend you take

Change your MangaDex password. While not compromised, this is always a good idea in such a situation. Similarly, change your password on other sites if it was reused.

Use a password manager. They allow you to generate secure randomized passwords for every website you use and in the event of breaches like this, means that your other accounts are safe. Most browsers offer this feature natively when you attempt to sign up for websites, but you can also use a separate program like Bitwarden which is free and open-source. You can also sync your passwords between devices, and if you use a standalone password manager, store credentials unrelated to websites.

Activate 2-factor authentication in your “Password and security” settings on MangaDex. If you had it enabled already, you will need to re-enable it again.

Update your email address. You might want to change email to one that is not tied to your school/workplace if that was the case before, as we’re not an official site after all.

Final thoughts

While it is unfortunate that this has occurred, remember that sites much larger than ourselves (which are professionally maintained) have also been breached before. If anything, this event has increased the urgency of finishing and releasing v5, which is professionally written, unlike the amateur code that is v3. Progress was going well on v5, but lately our attention was diverted to upgrading the infrastructure. As you will have noticed, since the upgrade, the site has been stable despite a surge of users yesterday from mangago being down. Our total throughput from MangaDex@Home reached as high as 38 Gbps compared to the usual average of 23 Gbps, something that wouldn’t have been possible even a month ago. A huge thanks to our new devops who have secured and are maintaining the new infrastructure. Finally, we would like to thank you all for being patient, supportive and understanding during this difficult time.