Issued 3/30/18

Security Flaw in Grindr Exposed Locations to Third-Party Service

Users of Grindr, the popular dating app, may have been broadcasting their location despite having disabled that particular feature. Two security flaws allowed for discovery of location data against a user's will, though they take a bit of doing. The first of the flaws, which were discovered by Trever Faden and reported first by NBC News, allowed users to see a variety of data not available normally: who had blocked them, deleted photos, locations of people who had chosen not to share that data and more. The catch is that if you wanted to find out about this, you had to hand over your username and password to Faden's purpose-built website, which would then scour your Grindr account for this hidden metadata. Of course it's a bad idea to surrender your credentials to any third party whatsoever, but regardless of that, this particular third party was able to find data that a user should not have access to in the first place. The second flaw involved location data being sent unencrypted, meaning a traffic snooper might be able to detect it. (In its comment, Grindr says it encrypts and obfuscates location data, but has not specifically denied the existence of this issue.) Grindr is a location-based app. Location is a critical element of our social network platform. This allows our users to feel connected to our community in a world that would seek to isolate us. That said, all information transmitted between a user's device and our servers is encrypted and communicated in a way that does not reveal your specific location to unknown third parties.