Issued 3/7/17

Twitter Vulnerability Allowed Hackers to Access Locked Accounts

Up until a few months ago, Twitter was affected by a serious vulnerability that could have allowed hackers to bypass the network's account locking mechanism. This account locking mechanism is something that Twitter uses when it detects suspicious behavior on a certain account, clues that might indicate that an account has been compromised.

The user needs to jump through a few hoops in order to get his or her account back. They need to confirm they are the legitimate owner by providing personal information, such as the phone number associated with the account and the email address. Aaron Ullger, security expert, says that things weren't really safe on Twitter until a few months ago. That's because he discovered a way to bypass this account locking mechanism by adding the targeted account to a mobile device. What he did was to add the locked account to his iPhone via the Settings page, install the Twitter app on the device, and was instantly given full access to the account. One thing remained the same, however - the targeted account remained locked on the Twitter website, so the bypass wasn't complete.

That wasn't too difficult to do, though, because via the iOS Twitter app, he could get access to the account's settings and get his hands on the very same email address and phone number Twitter demanded from an individual to confirm they were the true owners of the account. This pretty much means that a hacker who got a hold of someone's account could use this technique to force his way back into the account after Twitter locked them out. "An attacker with knowledge of a locked account's credentials would've been able to exploit the issue to gain complete access to the victim's profile," Ulger writes.