Warning: Apple device users need to immediately turn off this feature when not in use to avoid data disclosure

Security holes in the authentication of sending and receiving files through AirDrop on iOS devices could expose users' email and phone numbers.

Since 2019, the team of the Technical University of Darmstadt has sent to Apple the report on the poor security findings on its AirDrop feature. But so far, Apple has not made a move to fix it.

AirDrop is a feature that allows users to share files with Apple devices in the contacts. AirDrop uses a "mutual authentication mechanism" to compare the user's phone number, email with the phonebook of the other device, thereby verifying that someone is in the contact list or not.

Based on how this works, hackers can use "a device that is Wi-Fi capable and near the target" to "force" an Apple device with AirDrop on to authenticate, revealing the phone number. and email users who do not have the need to exchange data with any nearby machines.

Even though Apple encrypts that information, it uses a relatively weak hashing mechanism, so using simple techniques like brute-force attacks can reverse the hash value.

A report by the research team of the Technical University of Darmstadt also shows that about 1.5 billion Apple devices are likely to be attacked by an attacker to obtain personal information through AirDrop.

Currently, Apple has not yet offered a solution to completely overcome this problem. The team warns users to completely turn off AirDrop when there is no need to use it to ensure the safety of personal information.

You finished reading the article "**Warning: Apple device users need to immediately turn off this feature when not in use to avoid data disclosure**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
