All Bitcoin Wallets On Android "Vulnerable To Theft"

The Bitcoin (BTC) community has warned that due to a recently discovered critical weakness in Android's secure random number generator, every single Bitcoin wallet for Google's mobile OS is "vulnerable to theft".

Bitcoin.org has advised users to transfer all virtual currency from their mobile wallets to a new, secure Bitcoin address, not generated on a smartphone or tablet.

There have already been several reports of stolen BTC balances on Android devices. App developers have been notified, and are currently working to fix the problem.

Not so random

Bitcoins are a digital currency based on an open-source, peer-to-peer Internet protocol, first introduced in 2009 by an anonymous developer known under the alias 'Satoshi Nakamoto'. Bitcoins cannot be traced, and their ownership cannot be established. This has led to their popularity among certain Internet subcultures, anarchists and even real-world criminals. Recently, a number of major online businesses have started to accept BTC as a form of payment, improving its reputation.

The anonymous nature of Bitcoins means that in the event they are stolen, it's pretty much impossible to track down the thief or get them back.

On Sunday, Bitcoin.org reported the existence of a bug that allows wallets built on Android to reuse the same random number in the Bitcoin transaction signature. If this random number is ever used twice with the same private key, the key can be recovered, giving a third party access to the funds stored at the particular address.

The problem affects all Android wallets developed to date, including Bitcoin Wallet, blockchain.info, BitcoinSpinner, Andreas Schildbach Android Wallet and Mycelium.

In response, Bitcoin.org has instructed users to forward the balance to an alternative address not generated on Android. The website notes that apps which don't control the private keys are not affected: "For example, exchange frontends like the Coinbase or Mt Gox apps are not impacted by this issue because the private keys are not generated on your Android phone."

New Bitcoin wallet addresses can be generated for free in less than a minute, so the operation shouldn't be too difficult.

"If you use an Android wallet then we strongly recommended you upgrade to the latest version available in the Play Store as soon as one becomes available," concludes the statement.

Last week, a US federal judge had ruled that Bitcoins are a form of money and can be regulated by the authorities, while establishing whether Bitcoin Savings and Trust, the first alleged Ponzi scheme involving Bitcoins, falls under the jurisdiction of the US Securities and Exchange Commission.

What do you know about Bitcoin? Take our quiz!