

RANDOM THEFT —

All Android-created Bitcoin wallets vulnerable to theft

Android Java SecureRandom function flaw undermines security of Android wallets.

LEE HUTCHINSON - 8/12/2013, 3:15 PM



Bitcoin.org released a [security advisory](#) over the weekend warning the Bitcoin community that any Bitcoin wallet generated on any Android device is insecure and open to theft. The insecurity appears to stem from a flaw in the Android Java SecureRandom class, which under certain circumstances can