Bitcoin version 0.5.0 is now available for download at: http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoi
0.5.0/

The major change for this release is a completely new graphical interface that uses the Qt user interface toolkit.

This release include German, Spanish, Spanish-Castilian, Norwegian and Dutch translations. More translations are welcome; join the project at Transifex if you can help: https://www.transifex.net/projects/p/bitcoin/

Please report bugs using the issue tracker at github: https://github.com/bitcoin/bitcoin/issues

For Ubuntu users, there is a new ppa maintained by Matt Corallo which you can add to your system so that it will automatically keep bitcoin up-to-date. Just type “sudo apt-add-repository ppa:bitcoin/bitcoin” in your terminal, then install the bitcoin-qt package.

MAJOR BUG FIX (CVE-2011-4447)

The wallet encryption feature introduced in Bitcoin version 0.4.0 did not sufficiently secure the private keys. An attacker who managed to get a copy of your encrypted wallet.dat file might be able to recover some or all of the unencrypted keys and steal the associated coins.

If you have a previously encrypted wallet.dat, the first time you run bitcoin-qt or bitcoind the wallet will be rewritten, Bitcoin will shut down, and you will be prompted to restart it to run with the new, properly encrypted file.

If you had a previously encrypted wallet.dat that might have been copied or stolen (for example, you backed it up to a public location) you should send all of your bitcoins to yourself using a new bitcoin address and stop using any previously generated addresses.

Wallets encrypted with this version of Bitcoin are written properly.

Technical note: the encrypted wallet’s ‘keypool’ will be regenerated the first time you request a new bitcoin address; to be certain that the new private keys are properly backed up you should:

1. Run Bitcoin and let it rewrite the wallet.dat file
2. Run it again, then ask it for a new bitcoin address. Bitcoin-Qt: Address Book, then New Address… bitcoind: run the ‘walletpassphrase’ RPC command to unlock the wallet, then run the ‘getnewaddress’ RPC command.
3. If your encrypted wallet.dat may have been copied or stolen, send all of your bitcoins to the new bitcoin address.
4. Shut down Bitcoin, then backup the wallet.dat file. IMPORTANT: be sure to request a new bitcoin address before backing up, so that the ‘keypool’ is regenerated and backed up.

“Security in depth” is always a good idea, so choosing a secure location for the backup and/or encrypting the backup before uploading it is recommended. And as in previous releases, if your machine is infected by malware there are several ways an attacker might steal your bitcoins.

Thanks to Alan Reiner (etotheipi) for finding and reporting this bug.

MAJOR GUI CHANGES

“Splash” graphics at startup that show address/wallet/blockchain loading progress.

“Synchronizing with network” progress bar to show block-chain download progress.

Icons at the bottom of the window that show how well connected you are to the network, with tooltips to display details.

Drag and drop support for bitcoin: URIs on web pages.

Export transactions as a .csv file.

Many other GUI improvements, large and small.

RPC CHANGES

getmemorypool : new RPC command, provides everything needed to construct a block with a custom generation transaction and submit a solution

listsinceblock : new RPC command, list transactions since given block

signmessage/verifymessage : new RPC commands to sign a message with one of your private keys or verify that a message signed by the private key associated with a bitcoin address.

GENERAL CHANGES

Faster initial block download.