Bitcoin version 0.4.1 is now available for download at: http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoi
0.4.1/

This is a bugfix only release based on 0.4.0.

Please report bugs by replying to this forum thread.

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 wxbitcoin 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. wxBitcoin: new address visible on main window 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.