Bitcoin-Qt version 0.8.4 is now available from: http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.8.4/

This is a maintenance release to fix a critical bug and three security issues; we urge all users to upgrade.

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

How to Upgrade

If you are running an older version, shut it down. Wait until it has completely shut down (which might take a few minutes for older versions), then run the installer (on Windows) or just copy over /Applications/Bitcoin-Qt (on Mac) or bitcoind/bitcoin-qt (on Linux).

If you are upgrading from version 0.7.2 or earlier, the first time you run 0.8.4 your blockchain files will be re-indexed, which will take anywhere from 30 minutes to several hours, depending on the speed of your machine.

0.8.4 Release notes

Security issues

An attacker could send a series of messages that resulted in an integer division-by-zero error in the Bloom Filter handling code, causing the Bitcoin-Qt or bitcoind process to crash. Bloom filters were introduced with version 0.8, so versions 0.8.0 through 0.8.3 are vulnerable to this critical denial-of-service attack.

A constant-time algorithm is now used to check RPC password guess attempts; fixes https://github.com/bitcoin/bitcoin/issues/2838 (CVE-2013-4165)

Implement a better fix for the fill-memory-with-orphan-transactions attack that was fixed in 0.8.3. See https://bitslog.wordpress.com/2013/07/18/buggy-cve-2013-4627-patch-open-new-vectors-of-attack/ for a description of the weaknesses of the previous fix. (CVE-2013-4627)

Bugs fixed

Fix multi-block reorg transaction resurrection.

Fix non-standard disconnected transactions causing mempool orphans. This bug could cause nodes running with the -debug flag to crash.

OSX: use 'FD_FULLSYNC' with LevelDB, which will (hopefully!) prevent the database corruption issues many people have experienced on OSX.

Linux: clicking on bitcoin: links was broken if you were using a Gnome-based desktop.

Fix a hang-at-shutdown bug that only affects users that compile their own version of Bitcoin against Boost versions 1.50-1.52.

Other changes

Checkpoint at block 250,000 to speed up initial block downloads and make the progress indicator when downloading more accurate.

Thanks to everybody who contributed to the 0.8.4 releases!

Pieter Wuille Warren Togami Patrick Strateman pakt Gregory Maxwell Sergio Demian Lerner grayleonard Cory Fields Matt Corallo Gavin Andresen