Bitcoin Core version 0.9.4 is now available from:

https://bitcoin.org/bin/0.9.4/

This is a new minor version release, bringing only bug fixes and updated translations. Upgrading to this release is recommended.

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).

OpenSSL Warning

OpenSSL 1.0.0p / 1.0.1k was recently released and is being pushed out by various operating system maintainers. Review by Gregory Maxwell determined that this update is incompatible with the Bitcoin system and could lead to consensus forks.

Bitcoin Core released binaries from https://bitcoin.org are unaffected, as are any built with the gitian deterministic build system.

However, if you are running either

- The Ubuntu PPA from https://launchpad.net/~bitcoin/+archive/ubuntu/bitcoin
- A third-party or self-compiled Bitcoin Core

upgrade to Bitcoin Core 0.9.4, which includes a workaround, **before** updating OpenSSL.

The incompatibility is due to the OpenSSL update changing the behavior of ECDSA validation to reject any signature which is not encoded in a very rigid manner. This was a result of OpenSSL's change for CVE-2014-8275 "Certificate fingerprints can be modified".

We are specifically aware of potential hard-forks due to signature encoding handling and had been hoping to close them via BIP62 in 0.10. BIP62's purpose is to improve transaction malleability handling and as a side effect rigidly defines the encoding for signatures, but the overall scope of BIP62 has made it take longer than we'd like to deploy.

0.9.4 changelog

Validation:

- `b8e81b7` consensus: guard against openssl's new strict DER checks
- `60c51f1` fail immediately on an empty signature
- `037bfef` Improve robustness of DER recoding code

Command-line options:

- `cd5164a` Make -proxy set all network types, avoiding a connect leak.

P2P:

- `bb424e4` Limit the number of new addressses to accumulate

RPC:

- `0a94661` Disable SSLv3 (in favor of TLS) for the RPC client and server.

Build system:

- `f047dfa` gitian: openssl-1.0.1i.tar.gz -> openssl-1.0.1k.tar.gz
- `5b9f78d` build: Fix OSX build when using Homebrew and qt5
- `ffab1dd` Keep symlinks when copying into .app bundle
- `613247f` osx: fix signing to make Gatekeeper happy (again)

Miscellaneous:

- `25b49b5` Refactor -alertnotify code
- `2743529` doc: Add instructions for consistent Mac OS X build names

Credits

Thanks to who contributed to this release, at least:

- Cory Fields
- Gavin Andresen
- Gregory Maxwell
- Jeff Garzik
- Luke Dashjr
- Matt Corallo
- Pieter Wuille
- Saivann
- Sergio Demian Lerner
- Wladimir J. van der Laan

As well as everyone that helped translating on Transifex.