New issue

Jump to bottom

Security checklist #2218

Open ignopeverell opened this issue on 24 Dec 2018 · 3 comments

Labels enhancement help wanted

Milestone Mainnet

ignopeverell commented on 24 Dec 2018

Some feedback from the libsecp audit and our use in grin, all simple things we could add for a little more defense in depth:

- Zeroing of sensitive data through Drop (password, mnemonic)
- Check zeroing of private keys in libsecp
- More randomized tests to check invalid range proofs don't validate
- Same for aggsigs

ignopeverell added enhancement help wanted labels on 24 Dec 2018

ignopeverell added this to the **Mainnet** milestone on 24 Dec 2018

lehnberg mentioned this issue on 27 Dec 2018

Agenda: Development, Dec 27 #29 Closed

ghost commented on 28 Dec 2018

ignopeverell commented on 28 Dec 2018

Randomness was already checked, with rand 0.5+ it's fine.

This was referenced on 26 May 2019

Fill BlindingFactor with zeros on Drop #2847 Merged

Fill SecretKey with zeros on Drop for security mimblewimble/rust-secp256k1-zkp#51 Merged

yeastplume commented 25 days ago

Closing, out of date

yeastplume closed this 25 days ago

yeastplume reopened this 25 days ago

Assignees

No one assigned

Labels

enhancement

help wanted

Projects

None yet

Milestone

Mainnet

None yet

2 participants