A followup to my previous post Security concerns regarding token standards and $130M worth of ERC20 tokens loss on Ethereum mainnet - #17 by Dexaran

I made this post.

Here is a copy of the content poloniex_hacker_lost_funds.md · GitHub

It obviously got insta deleted from the subreddit. If someone can slap those reddit mods - please do it.

The post

Poloniex exchange was just hacked.

A hacker made this transaction https://etherscan.io/tx/0xc9700e4f072878c4e4066d1c9cd160692468f2d1c4c47795d28635772abc18db

And the tokens got permanently frozen in the contract of GLM! This shouldn't have happened if ERC-20 GLM token would be developed with security practices in mind. But ERC-20 still contains a security flaw that I discloser multiple times (here is a history of the ERC-20 disaster).

You can also find a full history of my fight with Ethereum Foundation over token standards since 2017 here ERC-223

The problem is described here.

Here is a security statement regarding the ERC-20 standard flaw: https://callisto.network/erc-20-standard-security-department-statement/

As of today, about $90,000,000 to $200,000,000 are lost to this ERC-20 flaw. Today we can increase this amount by $2,500,000.

The problem with ERC-20 token is that it doesn't allow for error handling which makes it impossible to prevent user errors. It was known for sure that the GLM contract is not supposed to accept GLM tokens. It was intended TO BE THE TOKEN, not to own the tokens. For example if you would send ether, NFT or ERC-223 token to the address of the said GLM contract - you wouldn't lose it.

Error handling is critical for financial software. Users do make mistakes. It's a simple fact. Whether it is misunderstanding of the internal logic of the contract, unfamiliar wallet UI, being drunk when sending a tx or panicking after hacking an exchange - doesn't matter. Anyone could be in a position of a person who just lost $2,5M worth of tokens to a simple bug in the software that could have been easily fixed.

I would use an opportunity to mention that ERC-223 was developed with the main goal of preventing such accidents of "funds loss by mistake: ERC-223: Token with transaction handling model

What is even worse - EIP process doesn't allow for security disclosures now. There is simply no way to report a security flaw in any EIP after its assigned “Final” status.

I'm proposing a modification to EIP process to allow for security disclosures here: Modification of EIP process to account for security treatments - #12 by Dexaran - Process Improvement - Fellowship of Ethereum Magicians

There are ongoing debates on submission of an informational EIP regarding the ERC-20 security flaw: ethereum-cat-herders/EIPIP#293

And the Informational EIP pull request: ethereum/EIPs#7915

We've built ERC-20 <=> ERC-223 token converter that would allow both standards to co-exist and eventually prevent the issue of lost funds ERC223 converter

Also my team is building a ERC-223 & ERC-20 compatible decentralized exchange that will also remove such a weird opportunity to lose all their life savings to a software bug from users: https://dex223.io/

If you are rich and worried about ERC-20 security bugs dealing damage to Ethereum ecosystem and ruining users days - welcome to our ERC-223 family. We stand for security. We don't let our users funds to be lost by mistake.