7/24/17

NEWS: $30 Million Stolen in Parity Multi-Sig Wallet Hack

On July 19, a hacker exploited a particular bug in the Parity multi-sig wallet, draining three large accounts to a total of $30 million worth of Ether and ERC-20 tokens.

Multi-sig wallets are digital wallets for storing digital currencies in which the funds can only be withdrawn if an agreed-upon number of key-holders (signatories) sign off on it. Many projects raising funds through token sales use multi-sig wallets to store contributions to be withdrawn at a later date or when certain objectives are met.

The exploit in question was not complex, but it allowed the hacker to effectively rewrite the settings of the multi-sig wallet and obtain complete access to the funds.

A group of white-hat hackers were notified of the theft in action. Since implementing a broad fix immediately was impossible, they decided to use the same exploit to drain the remaining vulnerable wallets with an estimated total of $150 million.

From the Etherscan page of the account holding the rescued funds:

“If you hold a multi-sig contract that was drained, please be patient. They will be creating another multi-sig for you that has the same settings as your old multi-sig but with the vulnerability removed and will return your funds to you there.”

While the rescued funds from the vulnerable wallets are safe, the $30 million from the three wallets can never be recovered.

It is important to note that the Parity wallet had gone through extensive development, testing, and auditing by professional developers. Mistakes are inherent in programming.

The Ethereum community and its swift coordination got ahead of the problem before it could become the single greatest hack in the digital currency space, supplanting the $50 million hack of the DAO that resulted in a hard-fork of the Ethereum blockchain.