On Wednesday, July 19th, 2017, an exploit was found in Parity's multisig wallets. This exploit allowed anyone to take control over said wallet and perform any regular function, including transferring ether and killing the wallet. The presale contract that was launched had a multisig wallet that was vulnerable: https://etherscan.io/address/0x63c0f17c1f72e1315e3d4f8a89a37d95f1314793#readContract

Due to the nature of the presale contract, it was impossible to change the contract owner or outgoing address where the funds are sent. Once we learned of this exploit, we suspended all advertising and contacted the White Hat Group as well as other key Ethereum experts on our next steps. We were given a contract to be used to buy out the remaining presale and end it all in one fell swoop, sadly, we were not able to secure enough funding to completely buy it out. In the interim, we had a server setup and running performing the following:

- Check if the presale contract is sold out. If it is, takeover the wallet, call endPreSale, and get the funds out of the wallet in one block.
- Check if the presale contract had < 1000 Ethereum left to sell. If it did, we'd call the aforementioned contract to buy it out, end the presale, and recover the funds in one block.
- Check if the current block is within 5 blocks of the presale ended. If it was, it would start sending commands to a contract to start the recovery process without the use of any extra funds.

Due to the exploit, we were unable to publicly announce anything since anyone could have come in and simply killed the multisig wallet, thus locking the funds in the contract forever. Instead, we contacted trusted parties to try and secure funds to try and buy the contract out.

At 10:15pm EST, July 24, 2017, the presale contract was sold out and drained in one block. At first, we assumed the party responsible was not working with our interests in mind and had come to the conclusion that the funds were lost. Several minutes later we received an email from a white hat hacker that submitted proof they had the funds and are willing to return them in full. We are still working with this person to secure the funds, but steps must be taken to ensure that both parties are who they say they are.

Regardless of your opinion of Ethereum, this only proves there are a lot of good people in the community that want to help out in any way they can. More updates to follow as we receive them.