Hacker earned $ 32,000 in 7 weeks by fixing a series of gaps in e-money projects

Over the past 7 weeks, white-hat hackers around the world have earned at least $ 32,150 through the successful fix of a series of security flaws that appear on popular electronic and blockchain platforms like TRON, Brave, EOS and Coinbase.

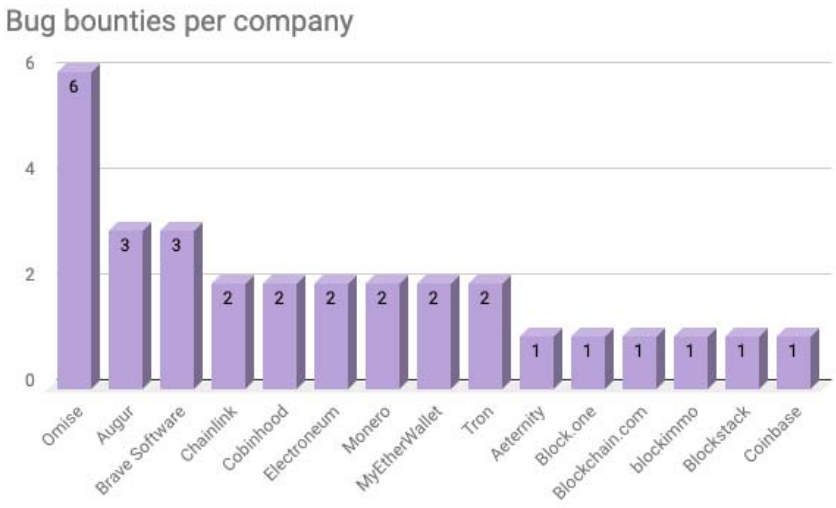
Over the past 7 weeks, white-hat hackers around the world have earned at least $ 32,150 through the successful fix of a series of security flaws that appear on popular electronic and blockchain platforms like TRON, Brave. , EOS and Coinbase.

According to Hard Fork statistics, a total of 15 companies operating in areas related to blockchain paid bonuses to security researchers between April 28 and May 16, with all 30 bug reports released publicly.

1. US $ 1.7 billion of electronic money was beaten by hackers in 2018

Omise, the software company behind the OmiseGo electronic currency, is the business that has released the most fixes (6 fixes). Ranked second is the market analyst Augur blockchain with three reports of error correction. Sharing the same position is a familiar name Brave Software, developer of the famous Brave security browser platform, owning its own token.

This bonus is collectively referred to as HackerOne, and projects have made adjustments to their HackerOne rewards depending on the severity of the detected security vulnerability. While most of Omise's bug fix reports are quite simple, and they are awarded an average of only $ 100 per report, the bonuses are spent on other organizations within the last 7 weeks. That number is very much because the hole they discovered is more complex and dangerous.



1. Detecting new electronic phishing malware, redirecting payment transactions to attackers

In particular, especially the case of Block.one, the company behind EOS's blockchain decided to reward a hacker with a record $ 10,000 with the discovery and successful repair of a security hole. Important confidentiality on your platform.

TRON has also paid $ 3,100 to a security researcher with another notable finding regarding the handling of malicious smart contracts, which may stall their blockchain platform.

This year, the number of white-hat hackers involved in fixing security issues seems to be stable compared to previous years. While the field of vulnerability exploitation has received more attention from security researchers.

In related information, Binance, one of the world's largest electronic money exchanges, said anonymous attackers successfully stole 7,000 BTC from their own wallet last week. This Bitcoin amount is equivalent to about 40 million dollars at the time of the incident, and now it has increased to 55 million dollars.

1. Stack Overflow hits the hacker face, no significant damage is recorded

Coincidentally, Binance is also organizing his own bug bonus program with a maximum reward of up to $ 100,000 for the most serious vulnerabilities.

The warming of the electronic money market in the past few months as a magnet attracted special attention from global hackers. Similar error-paying programs should be implemented more frequently and more aggressively to protect the overall security situation of the whole market.