Number	**Vulnerability**	**Cause**	**Level**
1	Call to the unknown	The called function does not exist	Contract source code
2	Out-of-gas send	Fallback of the callee is executed	
3	Exception disorder	Irregularity in exception handling	
4	Type casts	Type-check error in contract execution	
5	Reentrancy vulnerability	Function is re-entered before termination	
6	Field disclosure	Private value is published by the miner	
7	Immutable bug	Alter a contract after deployment	EVM bytecode
8	Ether lost	Send Ether to an orphan address	
9	Stack overflow	The number of values in stack exceeds 1024	
10	Unpredictable state	State of the contract is changed before invoking	Blockchain mechanism
11	Randomness bug	Seed is biased by malicious miner	
12	Timestamp dependence	Timestamp of block is changed by malicious miner	