**Miso:**

Miso is DeFI auction platform of Sushi. It allows creating a customized ERC20 token and deploy it to the blockchain. Then the user choose the auction type – DutchAuction / Crowdsale / BatchAuction. The DutchAuction

We review two files - DutchAuction.sol and BoringBatchable.sol.

“Dutch Auctions are a centuries old system of auction, aimed at finding the true market value of a completely novel item. In the case of MISO token auctions the price is set at a higher value per token than expected and descends over time, with the eventual price being settled on once all tokens have been sold.”

BoringBatchable.sol enables a user to call multiple functions at once, this is implemented in the “batch” function. This function loop over the input functions to call and at each applies a “delegatecall” method which keeps the state (msg.value in particular) while calling the function.

A picture containing text

Description automatically generated

The bug is that msg.value is counted multiple times, at each of the called function, without checking that the msg.value is already used.

For example, the user can call “commitEth” multiple time and get refund at each of the calls.

Graphical user interface, text, application, email

Description automatically generated

Each of the calls might have and the refund will be set to . The user will be refunded with total and can drain the contract.

**A simpler version of the bug:**

Imagine a bank contract with only two functions - deposit and withdraw. The contract use BoringBatchable.sol to allow multiple functions calls. One can call deposit multiple times, , using the function “batch” and have balance of .

Text

Description automatically generated