**ForceDAO Vulnerability:**

ForceDAO is a contract that allows customers do deposit funds and gain interest. The vulnerability isn’t related to the way they gain their interest, but rather ignoring the return value of the ERC20 contract methods (Boolean of fail / success) and allows the attacker to deposit and get tokens as much as he wants’ although the actual transfer failed.

The attacker can deposit any amount of funds and get a corresponding number of tokens, by depositing times the total balance of the contract, the attacker controls of the contract and can withdraw it. As the attacker transfer call fails, this is a pure profit for the attacker.

In contrast to many other attacks, this attack doesn’t involve a flash loan in order to manipulate the contract.

The used ERC20 implementation fixed this issue and now they revert instead of returning false - <https://github.com/Giveth/minime/commit/ea04d950eea153a04c51fa510b068b9dded390cb>.

Graphical user interface, text, application, Teams

Description automatically generatedThe vulnerable deposit function:

Text

Description automatically generatedThe called transferFrom: