




SECURITY SCANNER FOR ETHEREUM SMART CONTRACTS

 56918 Contracts scanned

 1740986 Issues found

STAY UPDATED

✓ Funded by an **Ethereum Foundation grant**.



✓ Created by **ICE center**, ETH Zurich and **ChainSecurity AG**, a top provider for smart contract audits.


LEARN MORE



<https://securify.chainsecurity.com/report/a8459bff0910b73ad311a2ad54b1a217664bb327f6a09733d4cda567b29d19be>



Share this report:

<https://securify.chainsecurity.com/report/a8459bff0910b73ad311a2ad54b1a217664bb327f6a09733d4cda567b29d19be> 

TOTAL issues 13

Recursive Calls 3

Reentrant method call

info



Method calls that are followed by state changes may be reentrant.

■ YieldContract: 601

■ YieldContract: 604

■ YieldContract: 628

Insecure Coding Patterns 4

Unrestricted write to storage

info



Contract fields that can be modified by any user must be inspected.

■ YieldContract: 588

■ YieldContract: 611

■ YieldContract: 626

■ YieldContract: 658

Unexpected Ether Flows 1

Locked Ether

info



Contracts that may receive ether must also allow users to extract the deposited ether from the contract.

■ YieldContract: 530

Dependence on unsafe inputs 5

Unsafe Call to Untrusted Contract

info



The target of a call instruction can be manipulated by an attacker.

■ YieldContract: 601

■ YieldContract: 604

■ YieldContract: 628

Repeated Calls to untrusted code

info



Repeated Calls to untrusted code might return inconsistent results.

■ YieldContract: 604

■ YieldContract: 628