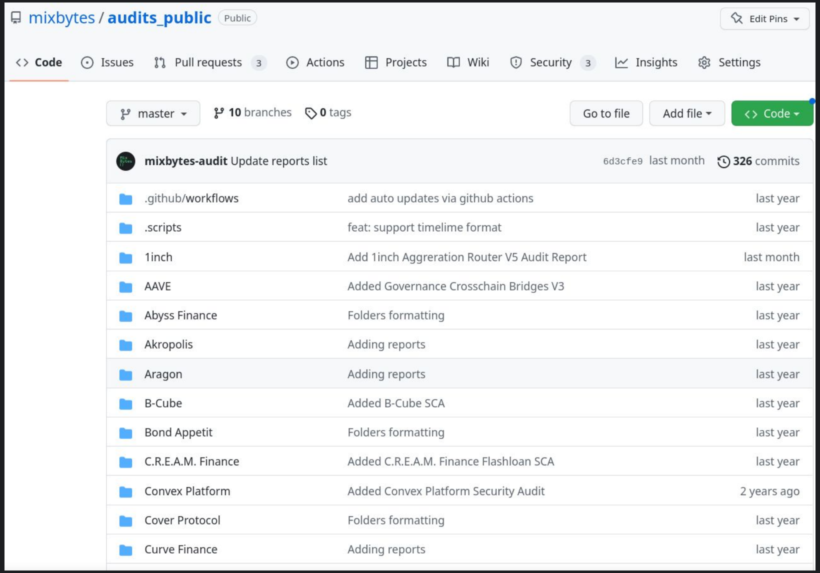
Mix
Bytes
()

Smart-Contract Auditor: From Zero to Hero

About MixBytes

- established in 2017;
- a leading global auditor, known for its diverse client portfolio;
- specializes on:
  - audits;
  - development;
  - edu & research;
  - consulting.



mixbytes-audit Update reports list 6d3cfe9 last month 326 commits

.github/workflows	add auto updates via github actions	last year
.scripts	feat: support timeline format	last year
1inch	Add 1inch Aggreration Router V5 Audit Report	last month
AAVE	Added Governance Crosschain Bridges V3	last year
Abyss Finance	Folders formatting	last year
Akropolis	Adding reports	last year
Aragon	Adding reports	last year
B-Cube	Added B-Cube SCA	last year
Bond Appetit	Folders formatting	last year
C.R.E.A.M. Finance	Added C.R.E.A.M. Finance Flashloan SCA	last year
Convex Platform	Added Convex Platform Security Audit	2 years ago
Cover Protocol	Folders formatting	last year
Curve Finance	Adding reports	last year

Mix
Bytes
()

Web3 Development

- open-source code;
- DAO & governance;
- bugfixes & hacks;
- bounties, grants and open-source support;
- public audits(!).

Auditor’s Profile

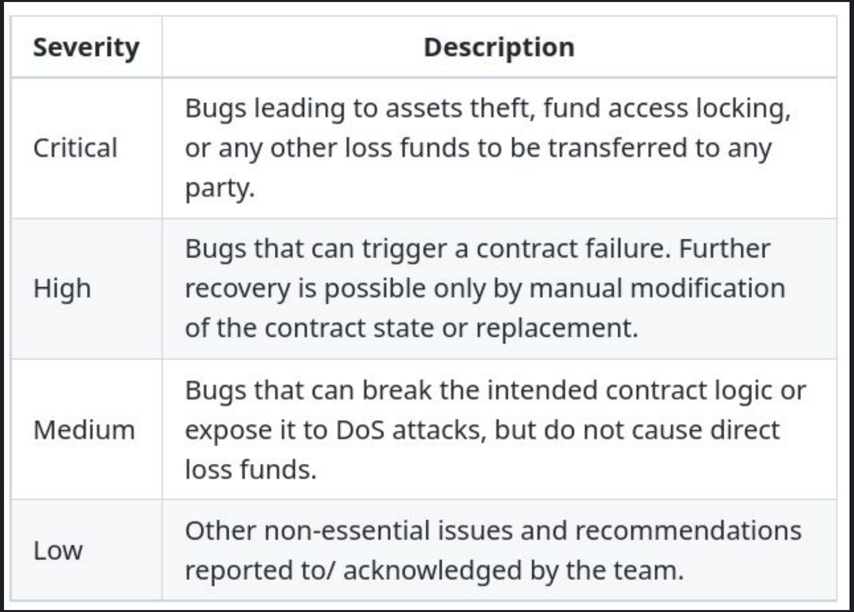
- critical thinking & attention;
- in-depth code examination;
- responsibility;
- strong technical background:
  - algorithms, data structures;
  - cryptography, security protocols;
  - maths, finances, economics, and data modeling;
  - information security, code analysis, pentesting;
  - experience with high-load, distributed systems, operating systems, and databases;
  - familiarity with various frameworks, tools, and software.

Tech Moments

- working with low-level code with higher-level understanding;
- a reduced instruction set and small executable code size;
- observable amount of logical branches;
- deep knowledge of protocols;
- many common security/financial patterns;

Inside the Workflow

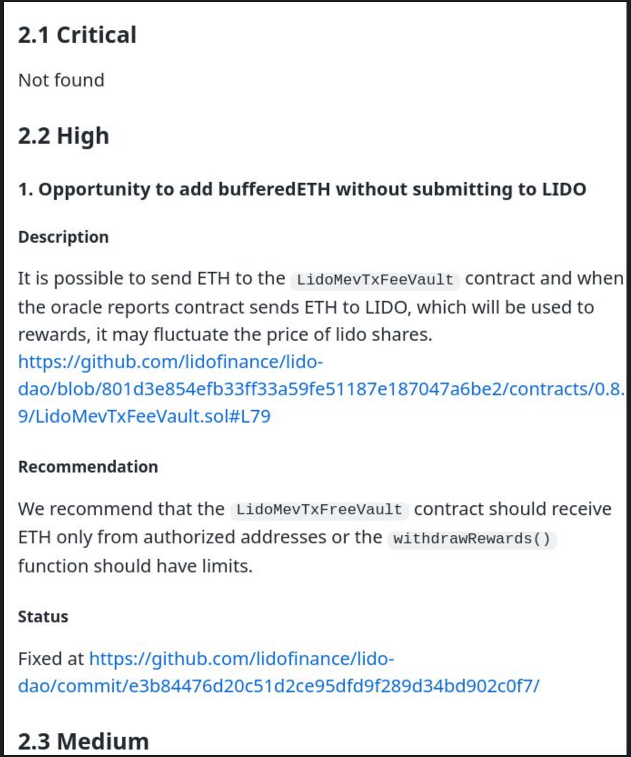
- scope definition;
- high-level protocol observation;
- audit plan;
- check code:
  - checklist approach;
  - similar projects cases;
  - own strategies.
- findings classification and validity;
- final review of findings;
- report.



Severity	Description
Critical	Bugs leading to assets theft, fund access locking, or any other loss funds to be transferred to any party.
High	Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.
Medium	Bugs that can break the intended contract logic or expose it to DoS attacks, but do not cause direct loss funds.
Low	Other non-essential issues and recommendations reported to/ acknowledged by the team.

Outside of the Workflow

- client: scope definition;
- auditors: estimation;
- auditors: audit;
- auditors: interim report;
- client: feedback from client devs:
  - reclassification of findings;
  - mitigation of findings.
- auditors: wait for all fixes;
- auditors: reaudit fixes;
- repeat until …;
- report



2.1 Critical

Not found

2.2 High

1. Opportunity to add bufferedETH without submitting to LIDO

Description

It is possible to send ETH to the `LidoMevTxFeeVault` contract and when the oracle reports contract sends ETH to LIDO, which will be used to rewards, it may fluctuate the price of lido shares. https://github.com/lidofinance/lido-dao/blob/801d3e854efb33ff33a59fe51187e187047a6be2/contracts/0.8.9/LidoMevTxFeeVault.sol#L79

Recommendation

We recommend that the `LidoMevTxFreeVault` contract should receive ETH only from authorized addresses or the `withdrawRewards()` function should have limits.

Status

Fixed at https://github.com/lidofinance/lido-dao/commit/e3b84476d20c51d2ce95dfd9f289d34bd902c0f7/

2.3 Medium

What to Audit

- full-featured audit;
- diff audit (for forks with changes);
- code review;
- setup/deploy continuous support;
- audit contests/bounty programs.

Mix
Bytes
()

How to Audit

- be ready for complex tasks;
- “word” is not enough evidence;
- avoid professional burnout;
- mix audits with research tasks:
    - examine hacks;
    - examine code analyzers;
    - write articles for the community;
    - share info between team members.

Who Audits?

- expert teams;
- solo security researchers;
- unfiltered crowd;
- DAOs conducting audits.

How to Enter?

- minimal set:
  - a strong understanding of Ethereum & blockchain technology;
  - Solidity/EVM low-level patterns;
  - Solidity high-level patterns;
  - a code review of important DeFi protocols ;
  - a deep understanding of typical vulnerabilities in DeFi;
  - comprehensive knowledge of various DeFi hacks and their implications.
- good to have:
  - passed CTF;
  - a test audit from scope to report.

Mix
Bytes
()

EOF

mixbytes.io

@MixBytes