1inch StepVesting Audit

5 May 2021, Igor Gulamov

Introduction

Igor Gulamov conducted the audit of 1inch StepVesting smart contract.

This review was performed by an independent reviewer under fixed rate.

Scope

StepVesting.sol

Issues

Major

1. https://github.com/1inch/governance-contracts/blob/97add372a6e183d8ad2bc7debd28359d5cd2f1ff/contracts/StepVesting.sol#L82

Claims will suspend if there will be not enough token in the contract. We propose replacing

```
    function available() public view returns(uint256) {
        return claimable().sub(claimed);
    }
```

with

```
    function available() public view returns(uint256) {
        return Math.min(
            claimable().sub(claimed),
            token.balanceOf(address(this))
        );
    }
```

or passing withdraw amout as `claim` parameter.

Severity Terms

Comment

Comment issues are generally subjective in nature, or potentially deal with topics like "best practices" or "readability". Comment issues in general will not indicate an actual problem or bug in code.

The maintainers should use their own judgment as to whether addressing these issues improves the codebase.

Warning

Warning issues are generally objective in nature but do not represent actual bugs or security problems.

These issues should be addressed unless there is a clear reason not to.

Major

Major issues will be things like bugs or security vulnerabilities. These issues may not be directly exploitable, or may require a certain condition to arise in order to be exploited.

Left unaddressed these issues are highly likely to cause problems with the operation of the contract or lead to a situation which allows the system to be exploited in some way.

Critical

Critical issues are directly exploitable bugs or security vulnerabilities.

Left unaddressed these issues are highly likely or guaranteed to cause major problems or potentially a full failure in the operations of the contract.