AUDITMOS

Secure your space

LOOP

audit / code review report

November 5, 2021

TABLE OF CONTENTS

1. License
2. Disclaimer
3. Approach and methodology
4. Description
5. Findings

contact@auditmos.com

AUDITMOS

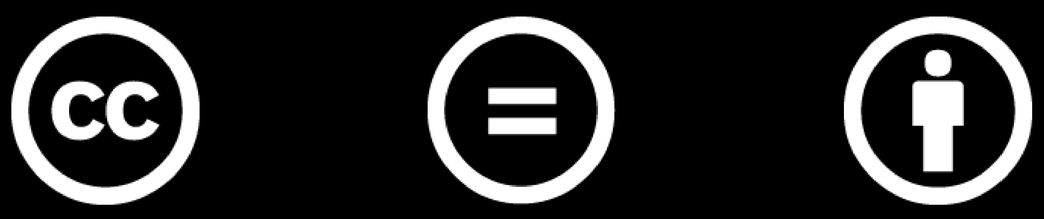
Secure your space

LOOP

audit / code review report

November 5, 2021

LICENSE



contact@auditmos.com

AUDITMOS

Secure your space

LOOP

audit / code review report

November 5, 2021

DISCLAIMER

contact@auditmos.com

AUDITMOS

Secure your space

LOOP

audit / code review report

November 5, 2021

APPROACH AND METHODOLOGY

PURPOSE

1. Determine the correct operation of the protocol, according to the design specification.
2. Identify possible vulnerabilities that could be exploited by an attacker.
3. Detect errors in the smart contract that could lead to unexpected behavior.
4. Analyze whether best practices were followed during development.
5. Make recommendations to improve security and code readability.

CODEBASE

Repository	https://github.com/Loop-Protocol/Loop_protocol_col5/tree/main
Branch	main
Commit hash	0f902abc1981be446445427d1fe2a75a2f28e161

METHODOLOGY

1. Reading the available documentation and understanding the code.
2. Doing automated code analysis and reviewing dependencies.
3. Checking manually source code line by line for security vulnerabilities.
4. Following guildlines and recommendations.
5. Preparing this report.

AUDITMOS

Secure your space

LOOP

audit / code review report

November 5, 2021

DESCRIPTION

Issues Categories:

Severity	Description
CRITICAL	vulnerability that can lead to loss of funds, failure to recover blocked funds, or catastrophic denial of service.
HIGH	vulnerability that can lead to incorrect contract state or unpredictable operation of the contract.
MEDIUM	failure to adhere to best practices, incorrect usage of primitives, without major impact on security.
LOW	recommendations or potential optimizations which can lead to better user experience or readability.

Each issue can be in the following state:

State	Description
PENDING	still waiting for resolving
ACKNOWLEDGED	know but not planned to resolve for some reasons
RESOLVED	fixed and deployed

contact@auditmos.com

AUDITMOS

Secure your space

LOOP

audit / code review report

November 5, 2021

FINDINGS

Finding	Severity	Status
#1 - Typo in response object	LOW	RESOLVED
#2 - Incorrect sender value	LOW	RESOLVED
#3 - General recommendations	LOW	RESOLVED

contact@auditmos.com

AUDITMOS

Secure your space

LOOP

audit / code review report

November 5, 2021

#1 - FIX IN RESPONSE OBJECT

There is a typo in response object

Severity	Status
LOW	RESOLVED

RECOMMENDATION

Replace below code

```
Ok(Response::new().add_attributes(vec![("last_distributed", "last_distributed")]))
```

with

```
Ok(Response::new().add_attributes(vec![("last_distributed",
last_distributed.to_string())]))
```

PROOF OF SOURCE

https://github.com/Loop-Protocol/Loop_protocol_col5/blob/0f902abc1981be446445427d1fe2a75a2f28e161/contracts/loops wap_farming/src/contract.rs

contact@auditmos.com

LOOP

audit / code review report

November 5, 2021

#2 - INCORRECT SENDER VALUE

It would be better to set sender to address of cw20 which sent that message.

Severity	Status
LOW	RESOLVED

RECOMMENDATION

Consider to change below code:

```
Ok(Response::new().add_messages(messages).add_attributes(vec![ ("action",
"staked"), ("sender", &sender.to_string()), ("receiver", &sender.to_string()), ]))
```

PROOF OF SOURCE

https://github.com/Loop-Protocol/Loop_protocol_col5/blob/0f902abc1981be446445427d1fe2a75a2f28e161/contracts/loops wap_staking/src/contract.rs#L290

LOOP

audit / code review report

November 5, 2021

#3 - GENERAL RECOMMENDATIONS

Follow the best practices writing your smart contracts in Rust

Severity	Status
LOW	RESOLVED

RECOMMENDATION

Consider to change below

```
let result_reward = REWARD_TOKEN_ISSUED.may_load(deps.storage,
key.clone())?; let mut reward_token_issued: Uint128 = Uint128::zero(); if
result_reward != None { reward_token_issued = result_reward.unwrap(); }
```

to

```
let reward_token_issued =
REWARD_TOKEN_ISSUED.load(deps.storage,key.clone()).unwrap_or(Uint128::zero()
);
```

PROOF OF SOURCE

https://github.com/Loop-Protocol/Loop_protocol_col5/blob/0f902abc1981be446445427d1fe2a75a2f28e161/contracts/loops wap_staking/src/contract.rs#L290

auditmos.com

AUDITMOS

Secure your space

contact@auditmos.com