StakeMyGold Audit Report

Prepared with Cyfrin

Version 2.0

Nov 17, 2025

Contents

1 About Cyfrin

Cyfrin is a Web3 security company dedicated to bringing industry-leading protection and education to our partners and their projects. Our goal is to create a safe, reliable, and transparent environment for everyone in Web3 and DeFi. Learn more about us at cyfrin.io.

2 Disclaimer

The Cyfrin team makes every effort to find as many vulnerabilities in the code as possible in the given time but holds no responsibility for the findings in this document. A security audit by the team does not endorse the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the solidity implementation of the contracts.

3 Risk Classification

	Impact: High	**Impact: Medium**	**Impact: Low**
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

4 Protocol Summary

The StakeMyGold is a staking platform for GGBR tokens where users can stake tokens for fixed lock periods and earn APRs that vary by lock duration. Users can create multiple stakes simultaneously, each with its own lock period and APR. Early withdrawals before the lock period expires are allowed but incur a penalty on accrued rewards, while withdrawals after the lock period ends receive full principal and rewards without penalty. The platform supports configurable staking periods, APRs, penalty rates, and minimum/maximum stake amounts, with administrative controls for managing these parameters.

This audit only concerned:

- StakeMyGold a manage contract that allows users to stake GGBR
- Reward calculation accuracy and precision in daily rate computations
- Access control for operator withdrawals and admin upgrade permissions
- Token balance tracking when withdrawing to or depositing from the ION wallet

General Overview:

Users can stake their GGBR token with specific lock period and APR.

Centralization Risks:

Due to the regulated nature of the underlying assets being tokenized and applicable regulatory requirements, the protocol is highly centralized by design including the ability for the protocol admins to seize the assets of users; users must place a high degree of trust in the protocol team. All issues related to centralization were outside the scope of the audit.

5 Audit Scope

The following contracts were included in the scope for this audit:

```
contracts/StakeMyGold.sol
```

6 Executive Summary

Our findings consisted of 1 Medium and 3 Low severity issues with the remainder being informational and gas optimizations.

All of the above findings were successfully mitigated by the protocol team.

Fuzz Testing:

As part of our audit we used both stateless and stateful/invariant fuzz testing; all code for our fuzz testing was delivered to the protocol team as an additional deliverable at the conclusion of the audit.

Summary

Project Name	StakeMyGold
Repository	StakeMyGold-smart-contracts
Commit	fad18ff2a51e8984799...
Audit Timeline	Nov 14th - Nov 17th
Methods	Manual Review, Cyfrin Aderyn

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	1
Low Risk	3
Total Issues	4

Summary of Findings

[M-1] StakeMyGold.sol has function to receive GGBR token but lacks a corresponding function to withdraw it, which leads to the GGBR being locked in the contract	Resolved
[L-1] nonReentrant is Not the First Modifier	Resolved
[L-2] State change without Event	Resolved
[L-3] Contract Name Reused in Different Files	Resolved

7 Findings

7.1 Medium Risk

7.1.1 StakeMyGold.sol has function to receive GGBR token but lacks a corresponding function to withdraw it, which leads to the GGBR being locked in the contract.

Description: It appears that the contract includes a receive function to accept GGBR but lacks a corresponding function to withdraw it, which leads to the GGBR being locked in the contract. To resolve this issue, we should implement a public or external function that allows for the withdrawal of GGBR from the contract.:

Impact: Token can be locked forever in contract.

Proof of Concept: Add this drop-in PoC to StakeMygold.sol :

```
// StakeMyGold.sol Line:802
function emergencyWithdraw(uint256 amount, address to) exernal onlyRole(DEFAULT_ADMIN_ROLE) {
    if (to == address(0)) revert ZeroAddress();
    if (amount == 0) InvalidAmount();

     ggbrToken.safeTransfer(to, amount);
}
```

StakeMyGold: Fixed in commit b7362e1

Cyfrin: Verified.

7.2 Low Risk

7.2.1 nonReentrant is Not the First Modifier

Description: To protect against reentrancy in other modifiers, the nonReentrant modifier should be the first modifier in the list of modifiers:

```
// nonReentrant is not the first Modifier
) external whenNotPaused nonReentrant returns
```

StakeMyGold: Fixed in commit 00e0956

Cyfrin: Verified.

7.2.2 State Change Without Event

Description: There are state variable changes in this function but no event is emitted. Consider emitting an event to enable offchain indexers to track the changes.

StakeMyGold: Fixed in commit c441c19

Cyfrin: Verified.

7.2.3 Contract Name Reused in Different Files

Description: When compiling contracts with certain development frameworks (for example: Truffle), having contracts with the same name across different files can lead to one being overwritten..

StakeMyGold: Fixed in commit ac62b7e

Cyfrin: Verified.