verichains

SECURITY AUDIT OF

ATHENA FOOTBALL TOKEN SMART CONTRACT

Public Report

Nov 03, 2022

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Nov 03, 2022. We would like to thank the Athena Football for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the Athena Football Token Smart Contract. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issue in the contract code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Athena Football Token Smart Contract

The Athena Football app is a mobile app created specifically for the world cup 2022, designed to help you experience every moment of this global event. Because they, the developers, are football fans, they decided to create a platform where all football fans can have fun by rooting for their favorite team.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Athena Football Token Smart Contract.

The audited contract is the Athena Football Token Smart Contract that deployed on Binance Smart Chain Mainnet at address `0x525B6dC1A1965200754054D4BF548E31E26e9503`. The details of the deployed smart contract are listed in Table 1.

FIELD	VALUE
Contract Name	AthenaFootballToken
Contract Address	0x525B6dC1A1965200754054D4BF548E31E26e9503
Compiler Version	v0.8.14+commit.80d49f37
Optimization Enabled	Yes with 200 runs
Explorer	*https://bscscan.com/address/0x525B6dC1A1965200754054D4BF548E31E26e9503*

Table 1. The deployed smart contract details

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.

- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 2. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure smart contract.

However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The Athena Football Token Smart Contract was written in `Solidity` language, with the required version to be `^0.8.14`. The source code was written based on OpenZeppelin's library.

2.1.1. Token contract

This is the ERC20 token contract in the Athena Football Token Smart Contract, which extends `ERC20Burnable`, `ERC20Pausable`, `AccessControlEnumerable`, `Context`, `SafeMath` contracts. `AccessControlEnumerable` implements role-based access control mechanisms. Contract deployer will be granted `DEFAULT_ADMIN_ROLE` and can set any roles for anyone. With `ERC20Pausable`, addresses with `PAUSER_ROLE` can `pause`/`unpause` contract, users can only transfer tokens when the contract is not paused. `ERC20Burnable` allows token holders to destroy both their own tokens and those that they have an allowance for.

The `DEFAULT_ADMIN_ROLE` can add/remove addresses to/from blacklist and blacklisted addresses can't send and receive tokens.

Table below lists some properties of the audited Athena Football token contract (as of the report writing time).

PROPERTY	VALUE
Name	Athena Football
Symbol	ATH
Decimals	18
Total Supply	100,000,000 ($x10^{18}$) Note: the number of decimals is 18, so the total representation token will be 100,000,000 or 100 million.

Table 3. Athena Football Token properties

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Athena Football Token Smart Contract.

2.3. Additional notes and recommendations

2.3.1. Use `calldata` instead of `memory` for gas saving INFORMATIVE

In `modifyBlackList` function with array arguments, using `memory` will force solidity to copy that array to memory thus wasting more gas than using directly from calldata. Unless you want to write to the variable, always using `calldata` for external function.

```
function modifyBlackList(
        address[] memory newBlackList,
        address[] memory removedBlackList
    ) public {
        require(
            hasRole(DEFAULT_ADMIN_ROLE, _msgSender()),
            "must have admin role to do function"
        );

        for (uint256 index; index < newBlackList.length; index++) {
            blackList[newBlackList[index]] = true;
        }
        for (uint256 index; index < newBlackList.length; index++) {
            blackList[removedBlackList[index]] = false;
        }
    }
```

RECOMMENDATION

Change `memory` to `calldata` for gas saving in all external functions.

APPENDIX

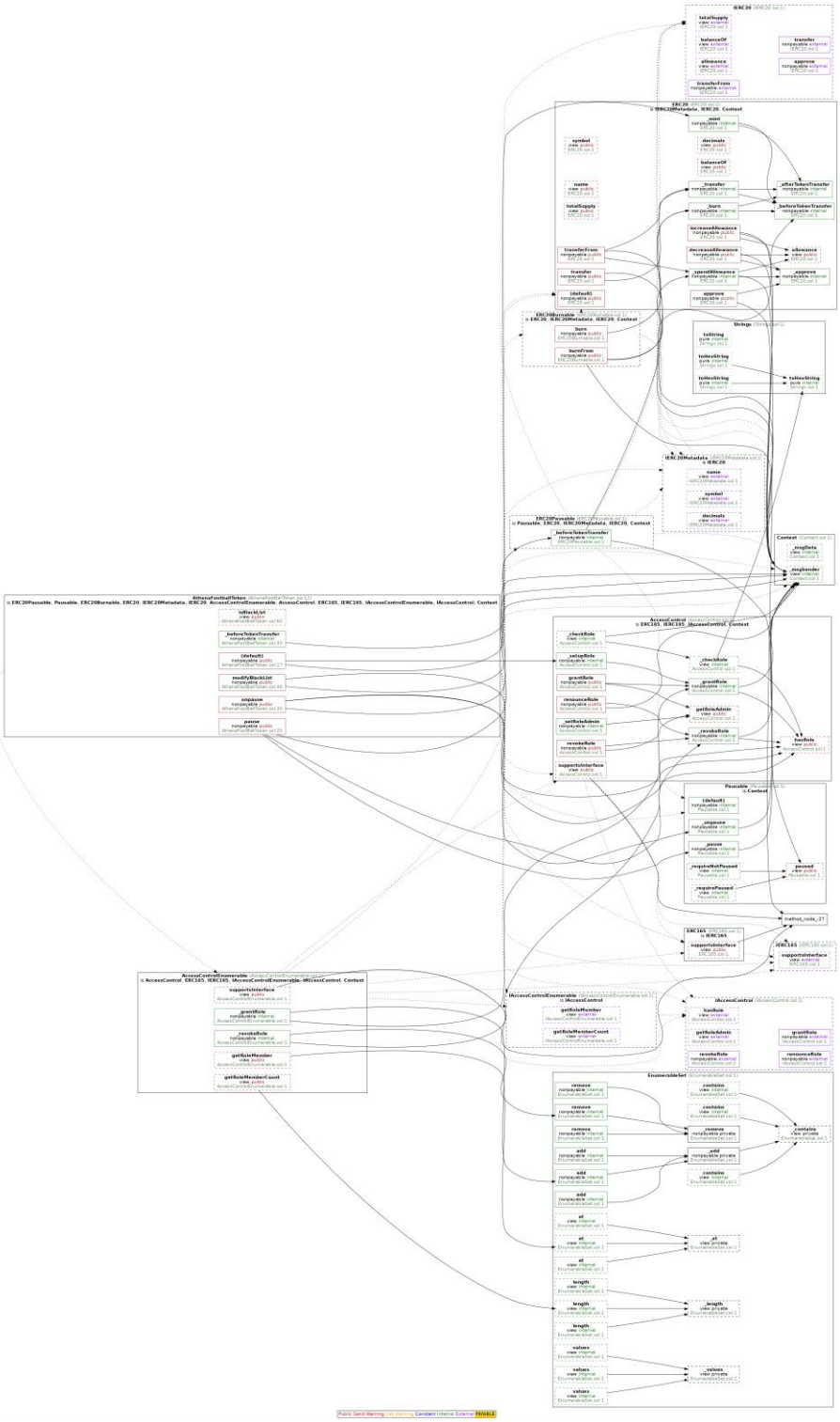

Image 1. Athena Football Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Nov 03, 2022*	Public Report	Verichains Lab

Table 4. Report versions history