verichains

SECURITY AUDIT OF

POLYSPORT TOKEN

Public Report

Mar 11, 2024

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 Mar 11, 2024. We would like to thank the Polysport 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 Polysport Token. 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 smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Polysport Token

Polysport Token is powered by Stark Finance with the development of blockchain technology and NFT, the NFT-based football game is becoming a new trend in the gaming world. Users can use Polysport Token to mint box, vote proposals and trade on marketplace.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Polysport Token that was deployed on Polygon.

The latest version was made available in the course of the review:

FIELD	VALUE
Address Deploy	0x860Ca4c7A60dCdc045BA1012c27788860cFa565f
Tx Deploy	0x6a3546abc68cdc5150fb7417790574a00de9442bef91d9efe3bc3c97862eb207
Deployer	0x4DcbFEC2bd337a9e863318898cd97539986a27f6
Block Number	53692547

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 1. Severity levels

1.4. Disclaimer

Polysport acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. Polysport understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Polysport agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the Polysport will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Polysport, the final report will be considered fully accepted by the Polysport without the signature.

2. AUDIT RESULT

2.1. Overview

The Polysport Token was written in `Solidity` language, with the required version to be `0.8.20`. The contract makes use of the `OpenZeppelin` library's `ERC20` extension. Below is the contract's properties:

PROPERTY	VALUE
Name	Polysport
Symbol	PLS
Decimals	18
Total Supply	$1,000,000,000 \times 10^{18}$ (It represents 1 billion tokens)

Table 2. The Polysport Token properties

For the ERC20 token, the security audit team has the following checklist of centralization standards:

Checklist	Passed
No Upgradeable	✅
No Fee modifiable	✅
No Mintable	✅
No Burnable	✅
No Pausable	✅
No Trading cooldown	✅
No blacklist	✅
No whitelist	✅

Table 3. The decentralization checklist

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Polysport Token.

APPENDIX
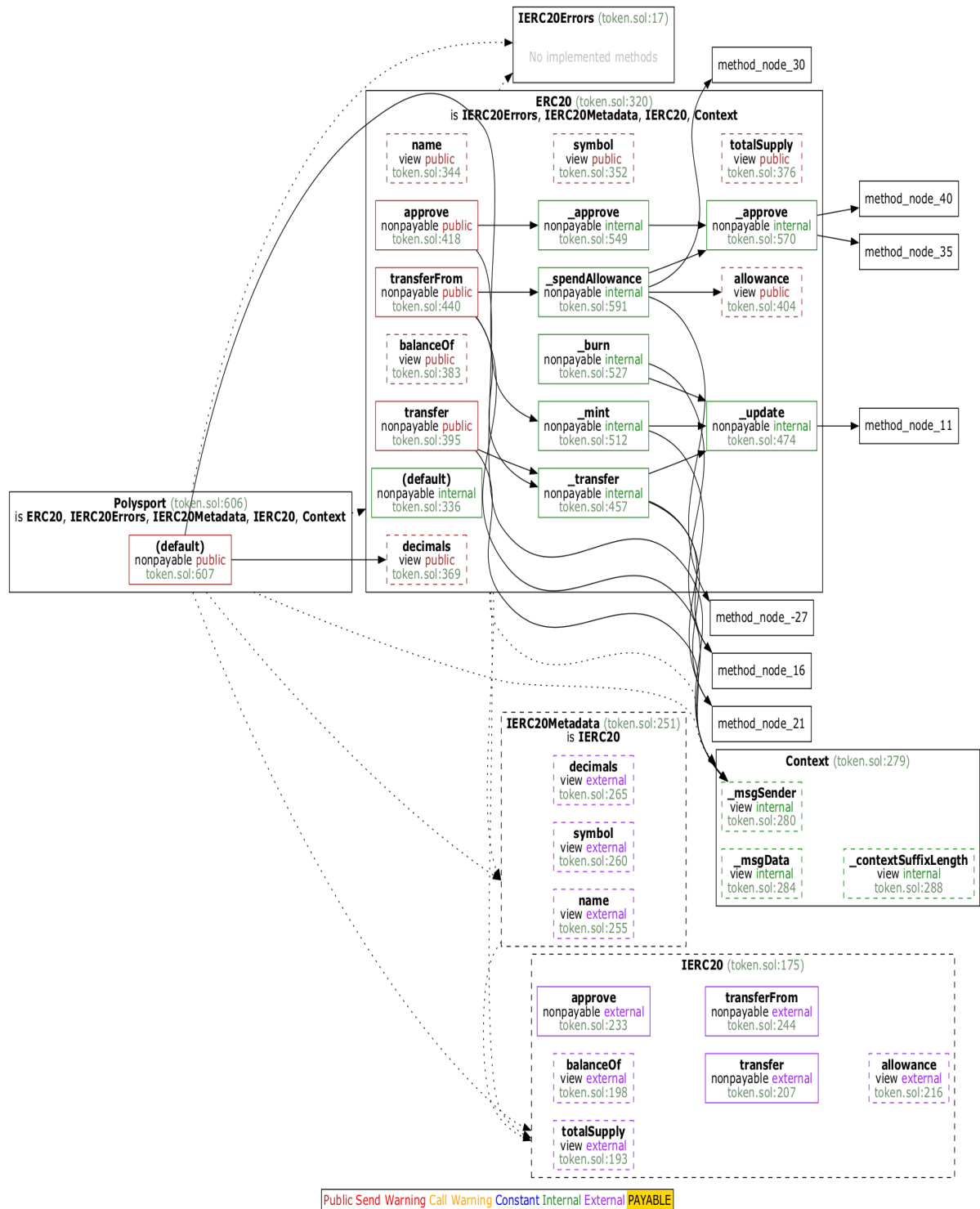
Image 1. ABI token smart contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Mar 11, 2024*	Public Report	Verichains Lab

Table 4. Report versions history