verichains

SECURITY AUDIT OF

SLS TOKEN SMART CONTRACT

Public Report

Nov 23, 2023

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 23, 2023. We would like to thank the SLS Token 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 SLS 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 vulnerability issue in the contract code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About SLS Token Smart Contract

SLS is a blockchain company, providing Web3 services for Enterprise to build a blockchain system connecting enterprises for Web3 (Enterprise Web3 Connector) to form the SLS ecosystem.

Validators in the SLS ecosystem will be able to use Web3 solutions (Web3 Enterprise Solution) to solve real-world problems, from finance to supply chain or even completely custom depending on business requirements.

SLS token is guaranteed by GVS GLOBAL ALLIANCE LLC - Headquartered in 99 Wall Street STE 3636 New York, NY 10005 - C.E.O KEVIN LAMPE.

SLS token is now trading on Bitmart.com.

1.2. Audit scope

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

The audited contract is the SLS Token Smart Contract that deployed on Ethereum Mainnet at address `0xEC537c4469Ff15811595a67dB0f6d7BD6131DED8`. The details of the deployed smart contract are listed in Table 1.

FIELD	VALUE
Contract Name	SLSToken
Contract Address	0xEC537c4469Ff15811595a67dB0f6d7BD6131DED8
Compiler Version	v0.8.5+commit.a4f2e591
Explorer	*https://etherscan.io/token/0xEC537c4469Ff15811595a67dB0f6d7BD6131DED8*

Table 1. The deployed smart contract details

1.3. Audit methodology

Our security audit process includes four steps:

- Mechanism Design is reviewed to look for any potential problems.

- Source codes are scanned/tested for commonly known and more specific vulnerabilities using public and our in-house security analysis tool.
- Manual audit of the codes for security issues. The source code is manually analyzed to look for any potential problems.
- Set up a testing environment to debug/analyze found issues and verifies our attack PoCs.

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 functioning; creates a critical risk to the application; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the application with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the application 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

SLS Token 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. SLS Token understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, SLS Token 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 SLS Token will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the SLS Token, the final report will be considered fully accepted by the SLS Token without the signature.

2. AUDIT RESULT

2.1. Overview

The SLS Token Smart Contract was written in `Solidity` language, with the required version to be `^0.8.0`.

2.1.1. SLSToken Token Contract

The `SLSToken` contract extends the `Ownable` contract. With `Ownable`, by default, the contract owner is the contract deployer, but he can transfer ownership to another address at any time. The contract defines two functions, `burn()` and `burnFrom()`, which allow users to burn their own tokens as well as tokens approved by others.

The smart contract is `ERC20` implementation that have some properties (as of the report writing time):

PROPERTY	VALUE
Name	SLS Connect Token
Symbol	SLS
Decimals	18
Total Supply	900,000,000 (x10^{18}) Note: the number of decimals is 18, so the total representation token will be 900,000,000 or 900 million.

Table 3. The SLS Token Smart Contract properties

For the ERC20 token, the security audit team has the list of centralization issues below:

Checklist	Status	Passed
Upgradeable	No	Yes
Fee modifiable	No	Yes
Mintable	No	Yes
Burnable	Yes	Yes

Checklist	Status	Passed
Pausable	No	Yes
Trading cooldown	No	Yes
Has blacklist	No	Yes
Has whitelist	No	Yes

Table 4. The decentralization checklist

2.2. Findings

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

Severity	Name	Status
INFORMATIVE	The redundancy of `Ownable` and `SafeMath` contracts	NEW

2.3. Additional notes and recommendations

2.3.1. The redundancy of `Ownable` and `SafeMath` contracts INFORMATIVE

- The `Ownable` contract is defined, but its functions are not used inside the contract.
- All safe math usages in the contract are for overflow checking, solidity `0.8.0+` already do that by default, the only usage of safemath now is to have a custom revert message which isn't the case in the auditing contracts. We suggest using normal operators for readability and gas saving.

APPENDIX

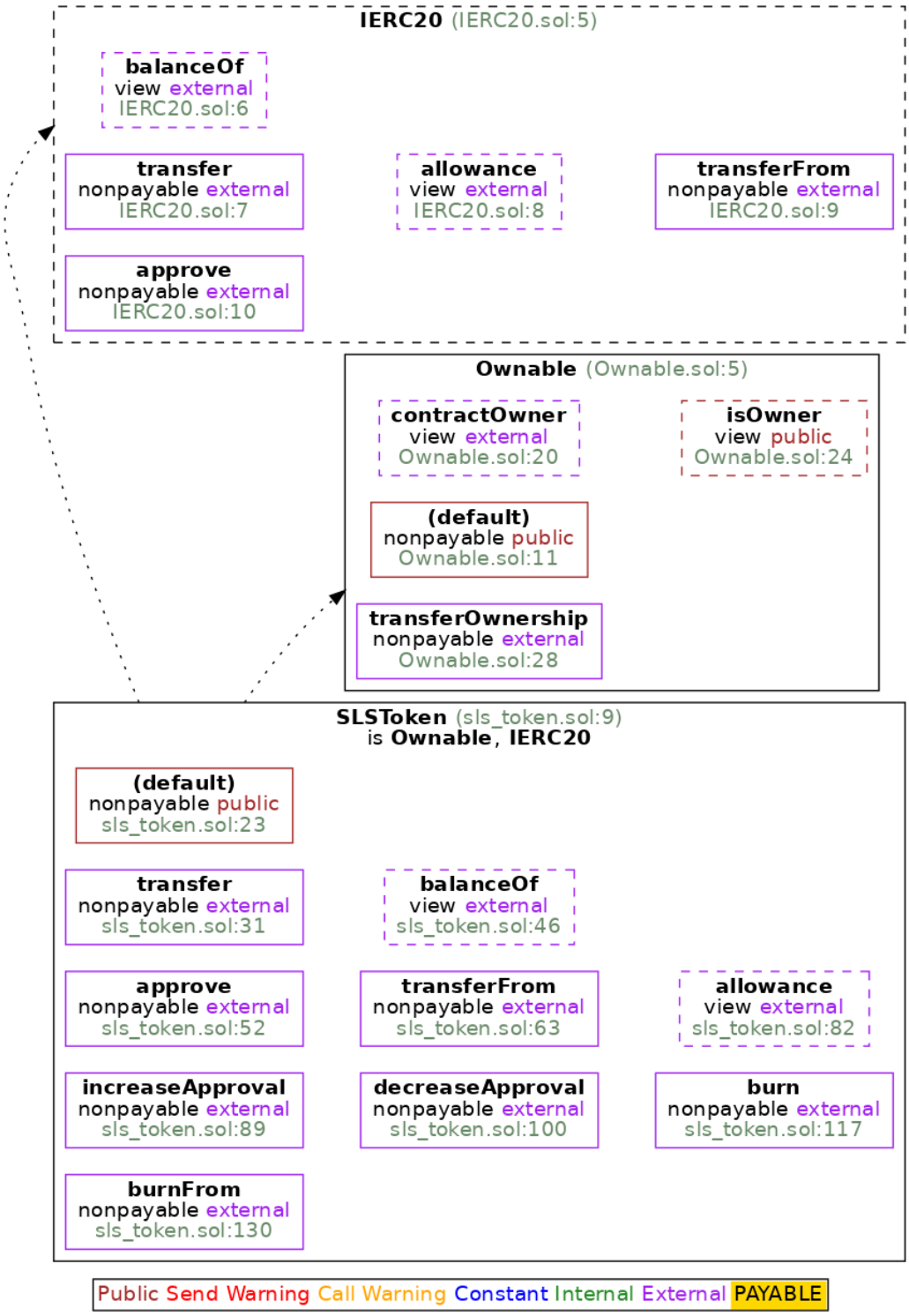

Image 1. SLS Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Nov 23, 2023*	Public Report	Verichains Lab

Table 5. Report versions history