shieldify

Sparta

SECURITY REVIEW

Date: 19 February 2025

CONTENTS

1. About Shieldify

Positioned as the first hybrid Web3 Security company, Shieldify shakes things up with a unique subscription-based auditing model that entitles the customer to unlimited audits within its duration, as well as top-notch service quality thanks to a disruptive 6-layered security approach. The company works with very well-established researchers in the space and has secured multiple millions in TVL across protocols, also can audit codebases written in Solidity, Rust, Go, Vyper, Move and Cairo.

Learn more about us at shieldify.org.

2. Disclaimer

This security review does not guarantee bulletproof protection against a hack or exploit. Smart contracts are a novel technological feat with many known and unknown risks. The protocol, which this report is intended for, indemnifies Shieldify Security against any responsibility for any misbehavior, bugs, or exploits affecting the audited code during any part of the project's life cycle. It is also pivotal to acknowledge that modifications made to the audited code, including fixes for the issues described in this report, may introduce new problems and necessitate additional auditing.

3. About Sparta

SPARTA ($SPARTA) is a hyper-deflationary token on Pulsechain that is closely linked to the performance of HEX.

The SPARTA system is simple: It has a 5% tax on buys and sells coupled with multiple high-volume trading pairs feeding into a common liquidity web. The fees from this volume strengthens liquidity and burns tokens.

4. Risk Classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

4.1 Impact

- **High** – results in a significant risk for the protocol's overall well-being. Affects all or most users
- **Medium** – results in a non-critical risk for the protocol affects all or only a subset of users, but is still unacceptable
- **Low** – losses will be limited but bearable – and covers vectors similar to griefing attacks that can be easily repaired

4.2 Likelihood

- **High** – almost certain to happen and highly lucrative for execution by malicious actors
- **Medium** – still relatively likely, although only conditionally possible
- **Low** – requires a unique set of circumstances and poses non-lucrative cost-of-execution to rewards ratio for the actor

5. Security Review Summary

The security review lasted 2 days and was conducted by the core Shieldify team of researchers.

Overall, the code is well-written. The audit report identified two low-severity vulnerabilities, along with one informational recommendation. The vulnerabilities primarily impact the contract initialization process and the tax/burn mechanism.

The Spart team has been highly responsive to the Shieldify research team's inquiries and promptly implemented all recommendations.

5.1 Protocol Summary

Project Name	**Sparta**
Repository	sparta-erc20
Type of Project	ERC-20
Audit Timeline	2 days
Review Commit Hash	3d42f456ad9ec82320bb8031a1766b4a49b8c43a
Fixes Review Commit Hash	3f443e25d36e4bf0144b5050e60c2c6afafad078

5.2 Scope

The following smart contracts were in the scope of the security review:

File	nSLOC
src/Airdrop.sol	50
src/Sparta.sol	134
src/Sparta.IPulseXPair	5
Total	**189**

6. Findings Summary

The following number of issues have been identified, sorted by their severity:

- **Low** issues: **2**
- **Informational** issues: **1**

ID	Title	Severity	Status
[L-01]	Value Of Sparta Can Be Affected If Malicious User Directly Deposits Into The Pair	Low	Fixed
[L-02]	Tax/Burn Can Be Evaded Through OTC Swaps	Low	Acknowledged
[I-01]	Tax Amount Cannot Be Changed	Informational	Acknowledged

7. Findings

[L-01] Value Of Sparta Can Be Affected If Malicious User Directly Deposits Into The Pair

Severity

Low Risk

Description

Between creating the contract and calling `init()`, anyone can directly deposit Hex into the UniswapV2 Pair.

The code mitigates this issue with `_fixV2PoolAndAddLiquidity()`, but note that if the Hex amount deposited is too high, the end value of Sparta may be lower than expected.

This would mean that the attacker purposely loses money to affect the value.

Location of Affected Code

Sparta.sol

```
// code

uint256 hexBalance = IERC20(hexToken).balanceOf(uniswapV2Pair);

if (hexBalance > 0) {
    _transfer(address(this), uniswapV2Pair, spartaLpAmount);
    IERC20(hexToken).transfer(uniswapV2Pair, hexLpAmount);

    IPulseXPair(uniswapV2Pair).mint(msg.sender, address(this));
}

// code
```

Impact

The price of SPARTA is lower than expected.

Proof of Concept

Assuming current price of HEX is 0.01198, and hacker deposits 85000e8 tokens ~$1000 USD directly into the pair

```
function testLP() external {
    address pair = sparta.uniswapV2Pair();

    deal(address(hexToken), user1, 85000e8);
    vm.startPrank(user1);

    console.log(address(pair));
    hexToken.transfer(pair, 85000e8);
    IPulseXPair(pair).sync();
    console.log(sparta.balanceOf(owner));
    _init_sparta2();
    console.log("Sparta", sparta.balanceOf(owner));
    console.log("HeX", hexToken.balanceOf(owner));
}

function _init_sparta2() internal {
    vm.startPrank(owner);

    uint256 initialHex = 83472e8;
    uint256 hexAmountToSwap = 5425709e8;
    deal(address(hexToken), owner, initialHex + hexAmountToSwap);
    hexToken.approve(
        address(sparta),
        initialHex + hexAmountToSwap
    );
    sparta.approve(address(sparta), INITIAL_SPARTA_LIQUIDITY);

    sparta.init(
        INITIAL_SPARTA_LIQUIDITY,
        initialHex,
        hexAmountToSwap,
        0,
        address(airdrop),
        AIRDROP_AMOUNT,
        block.timestamp
    );

    assertEq(sparta.balanceOf(treasuryWallet), 0);

    vm.stopPrank();
}
```

```
Reserve(0) (HEX): 559418100000000
Reserve(1) (SPARTA): 544985286579680306536966O2

1 HEX = 9.7420031025 SPARTA

Whereas if there is no deposit at all, pool reserves are:

Reserve(0) (HEX): 550918100000000
Reserve(1) (SPARTA): 27419923468460411251957960

1 HEX = 4.97713243919 SPARTA
```

Recommendation

Some ways to mitigate to ensure that the value of Sparta is controlled is to not swap so much Hex for Sparta, deposit lower amount of Sparta depending on how much is currently inside the pair and burn the rest, or depositing less amount of hex when creating the liquidity.

Team Response

Fixed.

[L-02] Tax/Burn Can Be Evaded Through OTC Swaps

Severity

Low Risk

Description

When a user buys / sells from an AMM pool, there is a buy tax / burn tax. Users can evade this tax by selling their sparta over the counter.

Users can also create other SPARTA/X pools , eg uniswap v3, and the protocol has to monitor all Sparta pools to set the pair address to allow tax.

Also, this will affect flash loans for the tokens.

Location of Affected Code

Sparta.sol

```
function _update(
    address from,
    address to,
    uint256 amount
) internal override {
    if (from == address(0) || to == address(0)) {
        super._update(from, to, amount);
        return;
    }

    if (blacklist[from] || blacklist[to]) revert Sparta__Blacklisted();

    if (taxEnabled) {
        uint256 taxAmount = (amount * BUY_SELL_TAX) / BPS;
        uint256 transferAmount = amount - taxAmount;
        super._update(from, to, transferAmount);

        if (isAmmPair[to]) {
            super._update(from, address(0), taxAmount);
        } else if (isAmmPair[from]) {
            super._update(from, treasuryWallet, taxAmount);
        } else {
            super._update(from, to, taxAmount);
        }
    } else {
        super._update(from, to, amount);
    }
}
```

Impact

Users can evade tax.

Recommendation

Just for acknowledgement as nothing much can be done with OTC swaps since transfers are not taxable.

Team Response

Acknowledged.

[I-01] Tax Amount Cannot Be Changed

Severity

Informational

Description

The `BUY_SELL_TAX` is set at a constant and cannot be changed.

Location of Affected Code

Sparta.sol

```
uint256 private constant BUY_SELL_TAX = 500;
```

Recommendation

There will forever be a 5% tax, and this value cannot be changed eg for events like attracting new investors/liquidity (0% tax etc).

Team Response

Acknowledged.

shieldify

Thank you!