SMC AUDIT

SMART CONTRACT
SECURITY AUDIT



AUDIT REPORT

Phoenix Token (PHT) Security Review

PROJECT	Phoenix Token (PHT)
CHAIN	BNB Chain (BSC, chain id 56)
CONTRACT	0x885c99a787BE6b41cbf964174C771A9f7ec48e04
DIVIDEND TRACKER	0xc541b47fB92Acc6e22dbd2bBC08439fE1E203A5E
VERSION	Deployed bytecode · Sourcify exact match (matchId 30594517) · solc 0.8.15
REPORT ID	SMC-PHT-202610-01
DATE	8 October 2026
PREPARED BY	SMC Audits
STATUS	Final

0 0

00 Confidentiality notice

This report is prepared by SMC Audits for the named project and contains confidential information, including identified security findings.

It should not be shared publicly until the project has remediated the issues described, and only with SMC Audits' agreement. Publication as part of public verification follows the process agreed in the engagement.

SMC AUDITS

01

01 Contents

02	Executive summary
03	Project overview
04	Scope
05	Methodology
06	Severity classification
07	Findings summary
08	Detailed findings
09	Remediation status
10	Conclusion
11	Disclaimer

SMC AUDITS

02

02 Executive summary

SMC Audits reviewed the Phoenix Token (PHT) smart contracts on BNB Chain at address 0x885c99a787BE6b41cbf964174C771A9f7ec48e04, using the source verified on Sourcify (an exact match of both creation and runtime bytecode, matchId 30594517).

The review covered the deployed PhoenixToken contract and the PhoenixTokenDividendTracker it deployed (0xc541b47fB92Acc6e22dbd2bBC08439fE1E203A5E) in full, including the fee, swap-back, burn, anti-bot, staking, dividend and administrative logic, cross-checked against live on-chain state, the token and LP locks, and the administrative history up to the renounce. The manual review, in four passes (owner and privileged powers, attacker view, line-by-line, severity challenge), was supported by 40 Foundry fork tests at BSC block 126,436,224 covering every finding, a read-only state-override eth_call that summed the dividend balances of all 8,780 tracked holders, and Slither 0.11.6 and Aderyn 0.6.8 with every medium-or-higher result triaged. All 40 tests pass.

The review identified 13 findings: 0 critical, 1 high, 2 medium, 2 low, and 8 informational. No issue lets an outside attacker take user funds. The most significant observation is that the renounced ownership does not make the token admin-free. The marketing wallet, a live EOA hardcoded in the constructor, receives BNB inside every sell that triggers the swap-back with all remaining gas, and under BSC's per-transaction gas cap of 16,777,216 (BEP-652, in force since 28 April 2026) a gas-burning EIP-7702 delegation on that wallet makes every taxed sell impossible until the wallet removes it (SMC-H-01, High). Separately, any holder can freeze every taxed sell for about 0.0013 BNB by driving the swap-back's fee counters to zero, and nobody can repair it (SMC-M-01, Medium), and 15.69% of supply sits in expired PinkLock locks held by three deployer-linked wallets that can be sold today (SMC-M-02, Medium).

The remaining findings are two low items (a permanent fee-exempt insider set and the approve race) and eight informational items. Overall, the fee split, burn, dividend accounting and rounding behave as written under the frozen configuration, and the dividend tracker is solvent. The token's integrity is contingent on the marketing wallet 0x1D28...abD3 never holding gas-burning code, a condition that is true today, that only that wallet's key holder can guarantee, and that can be changed in one transaction.

0	1	2	2	8	13
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL

As of this report, 0 of 13 findings have been resolved and verified by SMC Audits. The contracts are immutable and ownership is renounced, so the recommendations are advisory: they apply to the project

team, token holders, integrators and any future redeployment rather than to the live bytecode. Any residual risk is described in the conclusion.

03

03 Project overview

Phoenix Token (PHT) is a taxed BEP-20 dividend token on BNB Chain. This audit covers the single verified source file that implements the token (PhoenixToken), a 5% tax on buys and sells (1% burn, 1% marketing, 1% auto-liquidity, 2% holder rewards; wallet-to-wallet transfers are untaxed), an automatic swap-back through PancakeSwap V2, permanent anti-bot limits, an unused staking module, and the dividend tracker that pays holder rewards by swapping BNB into the payout token. The code is a widely used dividend-tracker template compiled with solc 0.8.15. Neither contract is a proxy or upgradeable.

System at a glance

COMPONENT	ROLE
PhoenixToken token contract	Balances, transfer / transferFrom, allowances. 10,000,000 PHT minted once (18 decimals), 9,530,714.30 reported as totalSupply today, no further mint.
Fee, burn and swap-back (in-contract)	Non-exempt buys and sells pay 4% to the contract and 1% to the dead address. A non-buy taxed transfer that finds at least 33.333 PHT in the contract turns 1/4 of the inventory into liquidity (LP minted to owner() = address(0)), sells the rest for BNB, and sends 2/3 of that BNB to the tracker and 1/3 to the marketing wallet. Buys are limited to 7 gwei gas, one per block per tx.origin and a 300,000 PHT wallet. Sells have a 60-second cooldown per tx.origin.
PhoenixTokenDividendTracker	Non-transferable dividend shares mirroring PHT balances of at least 1 PHT. 8,780 holders, 39.017 BNB distributed to date. Every taxed transfer processes holders for up to 300,000 gas. Its owner is the token contract.
Admin / ownership	owner() held every setter. Ownership was renounced to address(0) on 20 January 2024, so every owner function is dead. The marketing wallet 0x1D282C158038149f703aFb9237842FdD5139abD3 and the dev wallet (the deployer) are set in the constructor and have no setter.
External integrations	PancakeSwap V2 router and the PHT/WBNB pair, created in the constructor. The payout token, the Mudra LP locker, the PinkLock02 token locker, DEX contracts and market conditions are out of scope, but their live state was checked.

Key mechanisms to note

- Renouncing ownership did not remove every live privilege. owner() returns address(0) (renounce at block 35,411,114, 20 January 2024), and the tracker's owner is the token, so no admin function can run again. Three privileges survive because they never depended on owner(): the marketing wallet, paid with an unbounded-gas call inside every swap-back sell; 17 permanent fee exemptions, including the deployer and the marketing wallet; and four PinkLock02 token locks whose unlock dates have passed. These are the basis of SMC-H-01, SMC-L-01 and SMC-M-02.
- The 5% tax applies to pair trades only. Wallet-to-wallet transfers pay nothing. Only the PHT/WBNB pair is registered as a market and no other pool can ever be added, so trades through any other pool are untaxed (SMC-I-08).
- Liquidity is locked, part of the supply is not. 80.17% of the LP tokens are locked in the Mudra locker until 29 November 2030 and 19.83% sit at address(0). In contrast, PinkLock02 holds four PHT locks totalling 1,495,000 PHT (15.69% of supply) whose unlock dates passed between November and December 2025, while token trackers still show them as locked.

04

04 Scope

ITEM	DETAIL
Project	Phoenix Token (PHT)
Chain	BNB Chain (BSC, chain id 56)
Language	Solidity
Contracts	0x885c99a787BE6b41cbf964174C771A9f7ec48e04 (token) and 0xc541b47fB92Acc6e22dbd2bBC08439fE1E203A5E (dividend tracker, deployed by the token constructor), verified source via Sourcify.
Commit / version	Deployed bytecode; Sourcify exact match (matchId 30594517, verified 2026-06-03). Deployed at block 33,840,548 on 2023-11-26. Not a proxy.
Compiler	solc 0.8.15+commit.e14f2714, optimizer enabled (runs 200), EVM version london.

Files reviewed

FILE	LINES	NOTES
PhoenixToken.sol	2344	Entire file: Context, ERC20, SafeMath, Ownable, Uniswap V2 interfaces, DividendPayingToken, PhoenixToken, PhoenixTokenDividendTracker, IterableMapping. Token and tracker runtime bytecode rebuilt and matched byte for byte, except the metadata hash.

SMC AUDITS

Out of scope

Off-chain components, the project website and front end, and the payout token contract. Liquidity pools, DEX pairs, routers, token and LP lockers, and market or economic conditions. The PinkLock02 and Mudra lock states were read on-chain because they change the risk to holders. The Mudra locker is not verified, so its migrator path could not be reviewed (see Remediation status). Deployment process and key management history. No evidence gap affects a Critical, High, or Medium conclusion.

05

05 Methodology

Every SMC Audits review follows the same process, so the result means the same thing on every engagement.

1. Threat modeling. Understand what the contract does, where value moves, and who holds privilege.
2. Manual review. A line-by-line reading of the code by the audit team. This is the core of the work and where most issues are found.
3. Tooling. Static analysis and security tooling support the manual review, they do not replace it.
4. Proof of concept. Every material finding is confirmed with a working proof of concept rather than asserted.
5. Reporting. Findings are written up with severity, reproduction, and a clear recommendation.
6. Re-audit. Fixes are verified by the team to confirm the issue is closed without introducing a new one.

Review checklist

Access control, signer and owner checks; privilege and centralization risk; arithmetic, overflow, and precision; reentrancy and external call safety; token and supply logic, mint and burn; fee, tax, and reflection mechanics; approvals and allowance handling; oracle and price handling; upgradeability and proxy risk; pause, blacklist, and emergency switches; front-running and MEV exposure; denial of service and gas griefing.

06

06 Severity classification

SEVERITY	MEANING
CRITICAL	Direct loss of funds or full compromise, realistic to exploit

HIGH	Serious impact, exploitable under conditions a project would actually meet
MEDIUM	Meaningful risk, limited by conditions or the size of impact
LOW	Minor risk, hard to exploit or low in impact
INFO	Best practice and code quality notes worth addressing over time

07

07 Findings summary

ID	TITLE	SEVERITY	STATUS
SMC-H-01	Immutable marketing wallet can halt every taxed sell under BSC's per-transaction gas cap	HIGH	Open
SMC-M-01	Any holder can freeze every taxed sell through a zero fee-counter divisor	MEDIUM	Open
SMC-M-02	Expired PinkLock locks release 15.69% of supply to deployer-linked wallets	MEDIUM	Open
SMC-L-01	Permanent fee-, cooldown- and limit-exempt insider set	LOW	Open
SMC-L-02	ERC-20 approve race condition (SWC-114)	LOW	Open
SMC-I-01	Privileged functions rely entirely on renounced ownership	INFO	Acknowledged
SMC-I-02	Anti-bot limits are permanent and keyed on tx.origin	INFO	Open
SMC-I-03	Fee burn is counted twice in the total supply	INFO	Open
SMC-I-04	Dividend tracker behaviour and code quality	INFO	Open
SMC-I-05	Swap-back, payout and reinvest swaps use zero slippage limits	INFO	Open
SMC-I-06	Staking module is dead, and its latent logic is unsafe	INFO	Open

SMC AUDITS

SMC-I-07	Dividend reinvest buys tax-free and ignores the max wallet	INFO	Open
SMC-I-08	Trades through unregistered pools are untaxed and unlimited	INFO	Open

0	1	2	2	8	13
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL

08

08 Detailed findings

PoC note: fork tests run at BSC block 126,436,224 against the live bytecode. No live mainnet transaction was made. All 40 tests pass. The full tests are provided in the engagement materials.

SMC AUDITS

SMC-H-01 HIGH Open

Immutable marketing wallet can halt every taxed sell under BSC's per-transaction gas cap

CATEGORY

Privilege and centralization risk; denial of service and gas griefing

LOCATION

swapAndSendDividends(uint256) L1685-1744 (marketing payment L1733), _transfer swap-back L1523-1557, constructor L1055 (marketingWallet, no setter)

DESCRIPTION

When a non-exempt transfer that is not a buy finds at least swapTokensAtAmount (33.333 PHT) in the contract, _transfer runs the swap-back before moving the seller's tokens. swapAndSendDividends ends with `address(marketingWallet).call{value: marketingPayout}("")`, which forwards all remaining gas and ignores the result. marketingWallet is the EOA 0x1D282C158038149f703aFb9237842FdD5139abD3, written once in the constructor with no setter. Since BSC's Pascal hard fork (BEP-441) an EOA can give itself contract code with one EIP-7702 authorization and remove it later. A reverting delegate does no harm because the result is ignored. A gas-burning delegate does: under the 63/64 rule it consumes all but 1/64 of the gas left at the call, and the rest of the sell (the tracker's 300,000-gas processing loop, two dividend updates, the pair swap) needs about 500,000 gas. Since the Mendel hard fork (28 April 2026), BEP-652 implements EIP-7825 and rejects every transaction with a gas limit above 16,777,216. With at most about 253,000 gas left after the marketing call, the sell runs out of gas and reverts. The revert also undoes the swap-back, so the inventory never drains: every later non-exempt sell hits the same path, while buys keep working and keep adding inventory.

IMPACT

Holders cannot sell into the only liquid pool while buyers can still buy, which is the honeypot pattern. Adding liquidity is blocked as well. The non-exempt routes left are wallet transfers and pools the token does not know (SMC-I-08), where the only live alternative holds about $0.003, so there is no practical exit. Fee-exempt wallets, including the deployer, keep selling (SMC-L-01), and deployer-linked wallets hold 24.15% of supply, so combined with SMC-M-02 the stop gives insiders a one-way exit. Only the marketing key holder can arm or lift it, and nobody can repair the contract because the wallet has no setter and the token is not upgradeable. The switch is invisible to scanners that treat owner() == 0 as "no admin risk", and a normal sell simulation passes until the delegation is set. Rated High because the impact is a total sell block and it needs one authorization from a wallet the project controls. It is not Critical: it is not armed today (eth_getCode on 0x1D28...abD3 returns 0x at the fork block), it moves no holder's tokens, and a cheap forwarding or reverting delegate does not trigger it, so it cannot happen by accident.

PROOF OF CONCEPT

On a fork at block 126,436,224, vm.etch writes exactly the code an EOA has after a 7702 authorization. The minimum gas for a 1,000 PHT swap-back sell rises from 1,065,185 (no delegation) to 32,477,587 (gas-burning delegate), almost twice the cap. With the inventory at the trigger, a 1,000 PHT sell, a 1 PHT sell, a 10,000 PHT sell by the largest non-exempt holder and a direct transfer(pair, 1 PHT) all revert at 16,777,216 gas and succeed only at 40,000,000 gas. A

reverting delegate leaves sells working, a baseline swap-back sell fits at 2,000,000 gas, the fee-exempt deployer keeps selling during the halt, addLiquidityETH reverts at the cap, and removing the delegate restores the halted sell. From the live inventory, one ordinary 0.5 BNB buy lifts the inventory above the trigger and every taxed sell after it reverts, including the buyer selling back.

RECOMMENDATION

The live contract is immutable, no code fix is possible. The marketing wallet owner should publicly commit never to attach 7702 code to 0x1D28...abD3, keep that key in cold storage, and treat it as an admin key. Holders, trackers and listing sites should monitor eth_getCode on that address, where a 0xef0100... prefix means the halt can be armed. Future versions should pay fee receivers with a pull pattern, or with a gas-limited call whose failure is tolerated, never with unbounded gas inside the user transfer path, and keep fee receivers changeable by a timelocked multisig rather than hardcoded.

SMC AUDITS

SMC-M-01 MEDIUM Open

Any holder can freeze every taxed sell through a zero fee-counter divisor

CATEGORY

Denial of service and gas griefing; arithmetic, overflow, and precision

LOCATION

_transfer L1531-1537 and L1554-1575, swapAndSendDividends L1704 and L1712

DESCRIPTION

The swap-back splits the inventory by the running fee counters: `contractTokenBalance.mul(buyAmount).div(buyAmount + sellAmount)`, and again `address(this).balance.mul(buyAmount).div(totalAmount)`. The counters are reset to 0 after every swap-back and refilled by the fee of the transfer that follows. If they are both 0 while the inventory is at the trigger, every non-exempt transfer to the pair reverts with "SafeMath: division by zero". Any holder can produce that state: top the inventory up to 33.333 PHT with a plain transfer to the token (a fee-exempt recipient, so the counters do not move), transfer 1 wei to the pair so the swap-back runs and resets both counters while the 4% fee on 1 wei rounds to 0, then transfer 33.34 PHT to the token again. The next taxed sell divides by zero, and so does every sell after it until a taxed buy makes buyAmount non-zero. With ownership renounced, no parameter can be changed to avoid the division.

IMPACT

While frozen, every non-exempt holder's sell to the main pair and every liquidity add reverts, while buys and wallet transfers work and the 17 fee-exempt wallets keep selling. Any taxed buy lifts the freeze, but the attacker can re-arm it in one transaction after every buy for about 0.00134 BNB, roughly 0.042 BNB per day at the observed 31.3 buys per day. No funds are taken and the attacker gains nothing directly, the motive is griefing, making the token look like a honeypot, or letting exempt insiders exit first. Rated Medium: it needs no privilege, works on the live configuration and cannot be repaired, but it is limited by conditions. A contract that buys and sells in one transaction escapes, a wallet whose buy and sell land in the same block before the re-freeze can get out, and the attacker must keep paying with no return.

PROOF OF CONCEPT

Fork tests at block 126,436,224. The attacker spends 48.81 PHT to arm the freeze, after which a direct transfer to the pair and router sells by the largest non-exempt holder (284,370 PHT) and by a small holder revert with "SafeMath: division by zero", still one hour later with no buys. The fee-exempt marketing wallet sells 1,000 PHT during the freeze. A 0.01 BNB buy lifts it. Ten buy / re-freeze cycles cost 333.40 PHT (0.013455 BNB), with 10 of 10 sells attempted between buys reverting. A contract that buys and sells in one transaction escapes, addLiquidityETH reverts while frozen, and the smallest router sell that pays out leaves a non-zero counter.

RECOMMENDATION

The live contract is immutable, no code fix is possible. A frozen state is lifted by any taxed buy, so holders who see "SafeMath: division by zero" on a sell can buy a small amount and sell in the same block. Future versions should return early from the split when buyAmount + sellAmount ==

0, or split by the fee settings instead of the counters, and never rely on a divisor that a user transfer can zero.

SMC-M-02 MEDIUM Open

Expired PinkLock locks release 15.69% of supply to deployer-linked wallets

CATEGORY

Privilege and centralization risk; token and supply logic

LOCATION

Live state: PinkLock02 locks 1319250, 1319249, 1339874 and 1171111;
_isExcludedFromFees[devWallet] set in the constructor L1110

DESCRIPTION

PinkLock02 holds four PHT locks totalling 1,495,000 PHT (15.69% of the reported supply), all past their unlock dates: 450,000 PHT and 50,000 PHT (owner 0x5FE6...E035, unlock November and December 2025), 195,000 PHT (the deployer, 23 November 2025) and a 1,000,000 PHT vesting lock (0x5658...d9eb, fully vested, 800,000 PHT not yet withdrawn). None has been withdrawn, and each owner can withdraw in one transaction. The deployer is permanently fee-exempt, so its tokens arrive and can be sold without the 5% tax. The three owners are deployer-linked: the deployer owns one lock, created the others, and sent 0x5658...d9eb 500,000 PHT before launch.

IMPACT

The deployer alone can sell 195,000 PHT for 6.2234 BNB, removing 20.50% of the pool's BNB and cutting the price by 36.84%. If all three owners sell, they take 19.7403 BNB, 65.58% of the pool, and the price falls by 88.23%. Counting the other deployer-funded wallets (24.15% of supply), the pool loses 74.77% of its BNB and the price 93.72%. This is not a defect in the PHT code and the tokens belong to their owners, who pay the price impact, which is why it is not rated High. It is rated Medium because it needs no special condition, it is large, and holders are shown these tokens as "locked" by third-party trackers even though they are not.

PROOF OF CONCEPT

getLocksForToken on PinkLock02 returns the four locks with unlockedAmount 0, 0, 0 and 200,000 PHT, and a fork test releases 450,000, 50,000, 195,000 and 800,000 PHT at the fork timestamp. The deployer unlock-and-dump drains 2,050 bps of the pool for a 3,684 bps price fall, all three owners drain 6,558 bps, and the full insider dump of 2,301,700 PHT drains 7,477 bps of the pool for a 9,372 bps price fall.

RECOMMENDATION

The live contract has no code change that applies. The lock owners should relock the tokens with a new, published schedule, or send them to the dead address. Holders and listing sites should treat these four locks as unlocked supply held by deployer-linked wallets. Future versions should vest insider allocations linearly and remove insider fee exemptions before renouncing.

SMC-L-01 LOW Open

Permanent fee-, cooldown- and limit-exempt insider set

CATEGORY

Privilege and centralization risk; fee, tax, and reflection mechanics

LOCATION

constructor L1107-1111, setExcludeFees L1153-1156 (dead), _transfer L1460-1462

DESCRIPTION

17 addresses are fee-exempt forever: the token, the tracker, the marketing wallet, the deployer, PinkLock02 and 12 wallets exempted before the renounce. An exempt sender or recipient skips the whole fee block in _transfer: no 5% fee, no 1% burn, no 60-second cooldown, no max wallet, no gas-price check and no swap-back. The exemptions can never be removed.

IMPACT

Exempt wallets get a better price and no limits, and they are the only sellers that still work during SMC-H-01 and SMC-M-01. Their own balances are small today, so the direct impact is low. The importance is as the enabler of the asymmetric exits described in SMC-H-01, SMC-M-01 and SMC-M-02. It adds no harm on its own, hence Low.

PROOF OF CONCEPT

A 10,000 PHT sell returns 0.396225 BNB for an exempt wallet and 0.376660 BNB for a normal one, and the exempt wallet sells again in the same block while the normal wallet's second sell within 60 seconds reverts "cooldown period active". Exempt holders (excluding the token and tracker) hold 1,542,490.97 PHT, mostly in PinkLock02, and no exemption has ever been revoked.

RECOMMENDATION

The live contract has no code change that applies. Holders should treat these wallets as insiders with a privileged exit. Future versions should keep exemptions to the token, the tracker and the router path, and remove insider exemptions before renouncing.

SMC AUDITS

SMC-L-02 LOW Open

ERC-20 approve race condition (SWC-114)

CATEGORY

Approvals and allowance handling

LOCATION

approve(address,uint256) L266-274, transferFrom L276-291 (mitigations increaseAllowance / decreaseAllowance)

DESCRIPTION

approve overwrites the allowance. If an owner changes a non-zero allowance to another non-zero value, the spender can front-run the change, spend the old allowance and then spend the new one.

IMPACT

A spender can take up to the sum of both allowances. It needs a specific victim action plus a transaction-ordering advantage, and the contract already offers increaseAllowance and decreaseAllowance, hence Low.

PROOF OF CONCEPT

Alice approves Bob for 100 PHT, then tries to lower it to 50. Bob front-runs transferFrom(alice, bob, 100) and then spends the new 50, ending with 150 PHT against Alice's final intent of 50.

RECOMMENDATION

Immutable, no code fix. Holders and integrators should use increaseAllowance and decreaseAllowance, or set the allowance to 0 before a new value. Future versions should keep these helpers or support EIP-2612 permits with exact amounts.

SMC AUDITS

SMC-I-01 INFO Acknowledged

Privileged functions rely entirely on renounced ownership

CATEGORY

Privilege and centralization risk

DESCRIPTION

Every administrative function is onlyOwner. On the token, updateFees accepts up to 100% per side (its message says "15%") and leaves the burn fee uncapped, and other setters control exemptions, pairs, limits, the swap threshold, the payout token, dividend pausing and staking. The tracker's admin functions are onlyOwner with the token as owner. owner() is address(0), so none of these can run again. This is the main safety fact of the contracts and should be re-verified independently by any reader. It does not cover the non-owner privileges in SMC-H-01, SMC-M-02 and SMC-L-01.

CONDITIONAL SEVERITIES WITH A LIVE OWNER

FUNCTION	CAPABILITY	SEVERITY IF OWNER WERE ACTIVE
updateFees	Buy and sell tax up to 100% each, plus an uncapped burn	HIGH honeypot or fee seizure
setAutomatedMarketMakerPair, setLimitsInEffect, setcooldowntimer, setmaxWallet	Tax and cooldown any address as a pair, tighten limits	MEDIUM selective trading restrictions
updatePayoutToken, setDividendsPaused, setExcludeDividends	Redirect, pause or withhold holder rewards	MEDIUM reward manipulation
setExcludeFees, setPresaleWallet, transferAdmin	Create tax-free insider wallets	LOW unfair trading terms

IMPACT

None today (status Acknowledged, mitigated by the renounce). All 30 token owner functions and all 17 tracker owner functions revert for outside callers, confirmed against the live state and the admin history (renounce at block 35,411,114, 20 January 2024).

RECOMMENDATION

No action on the live contracts. Future versions should cap fees in the setter including the burn, bound limits, emit events for every configuration change, and use a timelocked multisig instead of renouncing if parameters still need to be managed.

SMC AUDITS

SMC-I-02 INFO Open

Anti-bot limits are permanent and keyed on tx.origin

CATEGORY

Denial of service and gas griefing; integration safety

DESCRIPTION

limitsInEffect is true and can never be turned off. Buys require a gas price of at most 7 gwei and at most one buy per block per tx.origin, sells have a 60-second cooldown per tx.origin, and the 300,000 PHT max wallet is checked on buys only. Wallet transfers bypass the max wallet. Removing liquidity through the router is treated as a taxed buy.

IMPACT

No loss. Users behind a shared tx.origin (relayers, bundlers, smart-wallet services) can block each other for a block or a minute, private bundles priced above 7 gwei cannot buy, and LP removals through the router pay 6% and revert above 300,000 PHT.

RECOMMENDATION

Integrators should send PHT trades from distinct origins and keep gas prices under 7 gwei. Future versions should key limits on the trading account, not tx.origin, and make anti-bot limits expire after launch.

SMC-I-03 INFO Open

Fee burn is counted twice in the total supply

CATEGORY

Token and supply logic, mint and burn

DESCRIPTION

The burn share of every taxed trade is moved to the dead address with super._transfer and is also subtracted from _totalSupply. Either step alone would record the burn, both together count it twice. The internal _burn is never used.

IMPACT

No balance is wrong, and nothing in the token or the tracker reads totalSupply. Since launch 469,285.70 PHT have been counted twice, so the sum of balances exceeds totalSupply by 4.92% and supply, market-cap and "burned" figures on explorers are distorted accordingly.

RECOMMENDATION

Data providers should compute supply from 10,000,000 minus the dead-address balance. Future versions should either transfer to the dead address or reduce the supply, not both.

SMC AUDITS

SMC-I-04 INFO Open

Dividend tracker behaviour and code quality

CATEGORY

Best practice / code quality; token and supply logic

DESCRIPTION

The dividend accounting is the standard magnified-dividend-per-share scheme and is solvent: the 1.147786 BNB it holds covers 0.336559 BNB owed to current holders, and the other 0.811227 BNB belongs to former holders who keep what they earned and are paid only if they call claim(). Other items: auto-liquidity is minted to owner() = address(0) (holder-positive, by accident), some access modifiers are mislabelled, comments and messages are wrong and template strings refer to other projects, every wallet-to-wallet transfer emits a zero-amount Transfer to the token, and the pragma floats (^0.8.15).

IMPACT

No loss. Former holders who sold out without claiming have 0.811227 BNB waiting that they may not know about. The rest affects integrations and monitoring only.

RECOMMENDATION

Holders should call claim() on the token before selling their last PHT. Future versions should pay out a holder's pending dividends when it leaves the list, fix the access modifiers, send auto-liquidity to a defined lock, pin the compiler and remove template leftovers.

SMC-I-05 INFO Open

Swap-back, payout and reinvest swaps use zero slippage limits

CATEGORY

Front-running and MEV exposure

DESCRIPTION

The swap-back sells with amountOutMin = 0 and adds liquidity with minimums of 0, and the tracker swaps each holder's BNB into the payout token (and, on reinvest, into PHT) with amountOutMin = 0. All use block.timestamp as the deadline.

IMPACT

Not profitable to exploit at current sizes. The swap-back fires as soon as the inventory reaches 33.333 PHT, so it never sells more than about 0.00134 BNB of PHT, and a sandwich pays the 5% tax twice. Measured front-running of a swap-back loses BNB on every size tested.

RECOMMENDATION

Nothing on the live contracts. Future versions should use reserve- or TWAP-based minimum outputs.

SMC AUDITS

SMC-I-06 INFO Open

Staking module is dead, and its latent logic is unsafe

CATEGORY

Token and supply logic; fee, tax, and reflection mechanics

DESCRIPTION

stakingEnabled is false and only the renounced owner could enable it, so stake always reverts. If it were enabled, the lock is only checked in the sell branch so staked tokens leave by a plain wallet transfer, that branch replaces the normal sell branch so sells pay no fee and no cooldown, the staking bonus multiplies dividend weight and outlives the lock, and because staking-mode sells add 0 to the fee counters a plain donation would arm the SMC-M-01 division by zero.

IMPACT

None on the live contract (unreachable). Relevant to anyone reusing this template.

RECOMMENDATION

None on the live contract. Future versions should remove the module or enforce the lock on every transfer, keep fees on staking-mode sells, and clear the bonus when the lock ends.

SMC-I-07 INFO Open

Dividend reinvest buys tax-free and ignores the max wallet

CATEGORY

Fee, tax, and reflection mechanics

DESCRIPTION

A holder that calls setReinvest(true) and then claim() has its dividends used by the tracker to buy PHT from the pair. The tracker is fee-exempt, so the buy pays no tax and skips the gas-price, one-buy-per-block and max-wallet checks, and the PHT is forwarded to the holder fee-free. Automatic reinvest is off, so this only happens on a manual claim.

IMPACT

Bounded by the holder's own dividends (the largest is 0.019843 BNB), no one loses principal. It lets a holder already at the 300,000 PHT max wallet keep growing it.

RECOMMENDATION

None on the live contract. Future versions should apply the buy tax and limits to reinvested amounts or route them through the normal buy path.

SMC AUDITS

SMC-I-08 INFO Open

Trades through unregistered pools are untaxed and unlimited

CATEGORY

Fee, tax, and reflection mechanics; integration safety

DESCRIPTION

Only the PHT/WBNB pair is registered in automatedMarketMakerPairs, and with the owner renounced no other pool can be added. Transfers to and from any other pool are treated as wallet transfers, which pay no fee and skip every anti-bot limit. A Pancake Infinity pool already exists with about $0.003 of liquidity.

IMPACT

No principal at risk. If volume moved to another pool, holders would lose their rewards, the burn and auto-liquidity from that volume, and traders would skip the anti-bot limits. It is also the only non-exempt route left during SMC-H-01, an impractical one at current depth.

RECOMMENDATION

Nothing on the live contract. Future versions should tax by default and whitelist wallets, or keep pair registration with a timelocked multisig.

09

09 Remediation status

After the project addresses the findings, SMC Audits re-audits the changes and records the outcome here. The reviewed contracts are immutable (not proxies) and ownership is renounced, so on-chain code changes are not possible. SMC-H-01 and SMC-M-02 can be reduced by the project team through actions outside the contract (key-management commitments for the marketing wallet, relocking or burning the PinkLock tokens). The rest is advisory, for holders, integrators and any future redeployment.

ID	SEVERITY	STATUS	VERIFIED FIX
SMC-H-01	HIGH	Open	None (immutable). Mitigation depends on the marketing wallet key holder, monitor eth_getCode(0x1D28...abD3).
SMC-M-01	MEDIUM	Open	None (immutable). Any taxed buy lifts a freeze.
SMC-M-02	MEDIUM	Open	None. Lock owners can relock or burn locks 1319250, 1319249, 1339874 and 1171111.
SMC-L-01	LOW	Open	None (immutable). Exemptions are permanent.

SMC AUDITS

SMC-L-02	LOW	Open	None (immutable). Mitigations in-contract (increaseAllowance / decreaseAllowance).
SMC-I-01	INFO	Acknowledged	Mitigated: powers neutralized by renounce to 0x0, verified live and in the admin history.
SMC-I-02	INFO	Open	None. Integration guidance.
SMC-I-03	INFO	Open	None (immutable). Data providers should use the dead-address balance.
SMC-I-04	INFO	Open	None. Former holders can still claim() 0.811227 BNB in total.
SMC-I-05	INFO	Open	None. Measured as unprofitable to sandwich.
SMC-I-06	INFO	Open	None. Unreachable, applies to future versions.
SMC-I-07	INFO	Open	None. Bounded by each holder's dividends.
SMC-I-08	INFO	Open	None. Applies to future versions.

Open items for completeness: the Mudra locker holding 80.17% of LP is not verified, so its migrator path could not be reviewed, which affects the LP-lock statement in Section 3 but no finding's severity. The EIP-7702 evidence for SMC-H-01 is a fork simulation of the post-authorization code, and Foundry does not apply BSC's 16,777,216 per-transaction gas cap, so the tests pass the cap explicitly as the call's gas, which is more than a real transaction can forward. Holder balances and dividend figures are at block 126,436,224 (8 October 2026).

10

10 Conclusion

At the reviewed address, Phoenix Token (PHT) is a dividend-tracker template token with a fixed 5% tax on pair trades, a PancakeSwap swap-back, permanent anti-bot limits and renounced ownership. The review found no critical issue. The fee split, burn, rounding and dividend accounting work as written, and the tracker is solvent.

The high and medium findings do not come from owner(), which is renounced and whose functions our live checks confirm are dead. They come from what the renounce leaves behind: the hardcoded

marketing wallet, which under BSC's per-transaction gas cap can stop every taxed sell through EIP-7702 and restart it at will (SMC-H-01); a swap-back divisor that any holder can zero for a fraction of a cent and that no one can repair (SMC-M-01); and expired locks that give deployer-linked wallets 15.69% of supply to sell (SMC-M-02). The remaining findings are two low and eight informational items, and none of them puts user funds at risk in the deployed state.

The load-bearing condition is that the marketing wallet 0x1D282C158038149f703aFb9237842FdD5139abD3 never holds gas-burning code. That condition is true today, but only that wallet's key holder can keep it true, and they can change it in one transaction. Readers should check eth_getCode on that address and the state of the four PinkLock02 locks themselves, and should not read "ownership renounced" as "no admin risk".

An audit reduces risk. It does not guarantee the absence of every vulnerability. Users and the project should treat this report as one part of a wider security practice.

11

11 Disclaimer

This report reflects the code reviewed at the specific commit or address stated in the scope, at the time of review. It does not cover changes made after the review, external dependencies outside the stated scope, off-chain components, or economic and market conditions. This report is not financial, investment, or legal advice. SMC Audits provides no warranty, express or implied, and accepts no liability for any loss arising from the use of the audited code. A clean report is not a guarantee of safety.

SMC AUDITS · CONFIDENTIAL · SMCAUDITS.COM

SMC AUDITS