SMC AUDIT

SMART CONTRACT
SECURITY AUDIT



AUDIT REPORT

Yukan (BuybackBabyToken) Security Review

PROJECT	Yukan (BuybackBabyToken)
CHAIN	BNB Chain (BSC, chain id 56)
TOKEN	0xd086B849a71867731D74D6bB5Df4f640de900171
DIVIDEND DISTRIBUTOR	0x660E6115a9f669d324c9F7e780bfD79a191F61bd
VERSION	Deployed bytecode · Sourcify exact match (matchId 42520190) · solc 0.8.4 · not a proxy
REPORT ID	SMC-YUKAN-202610-01
DATE	26 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 Yukan (BuybackBabyToken) smart contract on BNB Chain at address 0xd086B849a71867731D74D6bB5Df4f640de900171, using the source verified on Sourcify (an exact match of both creation and runtime bytecode, solc 0.8.4).

The review ran from 21 to 26 October 2026 and covered the deployed flattened token in full: Auth, DividendDistributor, the SafeMath, Address, Clones and IBEP20 helpers, the constructor, fee and swap-back logic, Zeus and auto-buyback, liquidity targeting, and the dividend wiring to the reward token DTG (0xb195...A1B6), cross-checked against live on-chain state, holder and lock scans, and the PancakeSwap V2 pair. The code is a PinkSale buybackBaby generator template (VERSION 2), not a bespoke protocol. The manual review, in four passes (privileged powers, adversarial outsider view, line-by-line with a creative hunt for missed edge cases, and a severity challenge against house standards) plus a confirmation rerun of the full proof suite, was supported by cast and Forge for live state, 62 Foundry fork tests at BSC block 128,976,460 covering every finding and every refuted candidate, and Sourcify for source and metadata verification. All 62 tests pass.

The review identified 17 findings: 0 critical, 1 high, 1 medium, 1 low, and 14 informational. The headline risk is a privileged-wallet sell halt: swapBack pays the marketing fee receiver with Solidity .transfer() (2,300 gas, reverts on failure). An EIP-7702 delegation on that receiver that reverts or burns more than the stipend bricks every non-exempt sell that triggers the swap-back, while buys keep working (SMC-H-01). Ownership reads as renounced to 0xdEaD, but the deployer remains permanently authorized and retains fee, receiver, exemption and buyback control up to the 25% cap (SMC-M-01). The approve race is the house Low (SMC-L-01). No outsider can freeze or drain the token under the live configuration, the fee-clear divide-by-zero candidate was closed with no finding, LP is 99.61% burned, and no material token or LP locks were found.

0	1	1	1	14	17
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL

As of this report, 0 of 17 findings have been resolved and verified by SMC Audits. The contract is immutable and the owner slot is dead, so recommendations are advisory for the deployer key holder, token holders, integrators and any future redeployment. Residual risk is described in the conclusion.

03

03 Project overview

Yukan is a taxed BEP-20 reflection token on BNB Chain. Pair trades pay a 4% fee split (1% liquidity, 0.5% buyback, 0.5% reflection, 2% marketing; denominator 10,000). Collected inventory is swapped back automatically: marketing BNB is sent to the fee receiver, liquidity is added when below the target, reflection BNB is deposited into the DividendDistributor for DTG rewards, and the buyback share remains as BNB in the token until an authorized Zeus or auto-buyback burns tokens to 0xdEaD. The flattened source is a PinkSale buybackBaby template compiled with solc 0.8.4. Neither the token nor the distributor is a proxy.

System at a glance

COMPONENT	ROLE
BuybackBabyToken (0xd086...0171)	Balances, allowances, fees, swap-back, Zeus/auto-buyback, liquidity targeting, Auth. Supply 1,000,000 YUKAN (18 decimals), minted once, no further mint.
DividendDistributor (0x660E...61bd)	Magnified dividends-per-share over DTG; onlyToken deposit/setShare/process; holders claim DTG. ~7,958 non-exempt shareholders at the fork block.
Auth (Safemoon-style)	owner slot and authorizations mapping. Deployer set owner and authorized at construction; owner later moved to 0xdEaD without clearing the bitmap.
Admin surface	authorized: fees (≤25%), fee receiver, fee/dividend exemptions, buyBacker flag, swap threshold, target liquidity, distributor gas, auto-buyback, Zeus, multiplier. onlyOwner (dead): authorize, unauthorize, transferOwnership, setDistributionCriteria.
External integrations	PancakeSwap V2 router 0x10ED...024E, pair YUKAN/WBNB 0x0797...8C7f (~15.0 BNB and ~3.88e22 raw YUKAN at the fork block). Reward token DTG 0xb195...A1B6 (renounced, 9% fee-on-transfer). Market conditions out of scope; live state was read.

Key mechanisms to note

- Ownership is renounced in name only. isOwner(0xdEaD) is true and onlyOwner paths are dead, but isAuthorized(deployer) remains true forever because unauthorize is onlyOwner. The deployer can still set fees to 25%, change the marketing receiver, exempt wallets, and spend contract BNB via Zeus (SMC-M-01).
- Marketing is paid with .transfer(). Failed payments revert the whole swapBack and therefore the user sell. Combined with EIP-7702, that is SMC-H-01. setSwapBackSettings cannot set swapEnabled to false, so the trigger path cannot be switched off.
- Liquidity is almost entirely burned. About 99.61% of LP sits at 0xdEaD; PinkLock and other known lockers hold none for the token or the LP. The expired-lock Medium standard does not apply.
- Holder rewards depend on DTG. Reflection BNB is swapped to DTG inside the distributor. DTG takes a fixed 9% fee-on-transfer; claims credit full unpaid earnings while holders receive about 91% (SMC-I-04).

04

04 Scope

ITEM	DETAIL
Project	Yukan (BuybackBabyToken)
Chain	BNB Chain (BSC, chain id 56)
Language	Solidity
Contracts	0xd086B849a71867731D74D6bB5Df4f640de900171 (token) and the distributor it deployed at 0x660E6115a9f669d324c9F7e780bfD79a191F61bd; verified source via Sourcify.
Commit / version	Deployed bytecode; Sourcify exact match of creation and runtime bytecode (matchId 42520190, verified 2026-07-17). Deployed at block 28,517,978 on 2023-05-25 by 0x40A7a27BeE7b9b1D1Cf5bfe8865BfB17bB2b541a. Not a proxy.
Compiler	solc 0.8.4+commit.c7e474f2; optimizer enabled (runs 200); EVM version istanbul; no libraries; no immutables.

Files reviewed

FILE	LINES	NOTES
BuybackBabyToken.sol (flattened)	1,755	Auth, DividendDistributor, BuybackBabyToken VERSION 2, OZ SafeMath/Address/Clones, IBEP20. SHA-256 f70dfb0b...44b96b.

A local build of the verified source matches the on-chain runtime bytecode byte for byte apart from the CBOR metadata hash; Sourcify reports exact creation and runtime matches.

Out of scope

Off-chain components, the project website and front end. The DTG token beyond its effect on claims, PancakeSwap contracts, and market or economic conditions; their live state was read because they change the risk to holders. Deployment process and key management history beyond what is visible on chain. 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	Marketing fee receiver can halt taxed sells via EIP-7702 and .transfer()	HIGH	Open
SMC-M-01	Cosmetic renounce leaves the deployer permanently authorized	MEDIUM	Open
SMC-L-01	ERC-20 approve race condition (SWC-114)	LOW	Open
SMC-I-01	Anyone can trigger swapBack; router calls use zero slippage	INFO	Open
SMC-I-02	SwapBack sandwich is unprofitable at the live threshold	INFO	Open
SMC-I-03	Zeus buyback sandwich can profit at large authorized size	INFO	Open
SMC-I-04	DTG reward token takes 9% fee-on-transfer on claims	INFO	Open
SMC-I-05	Shareholder dust-grief raises gas without a durable sell freeze	INFO	Open
SMC-I-06	Transfers to the zero address are allowed; supply is not reduced	INFO	Open
SMC-I-07	_totalSupply infinite-allowance sentinel never decrements	INFO	Open
SMC-I-08	Emptying the pair would brick sells at roughly the pool BNB cost	INFO	Open
SMC-I-09	Buyback-fee BNB accumulates in the token until Zeus or auto-buyback	INFO	Open
SMC-I-10	buyBacker mapping does not gate Zeus; authorized does	INFO	Open
SMC-I-11	setIsFeeExempt is one-way	INFO	Open
SMC-I-12	setSwapBackSettings cannot disable swapBack	INFO	Open
SMC-I-13	Circulating supply of zero bricks swapBack sells	INFO	Open
SMC-I-14	Over-liquified state skips auto-liquidity (by design)	INFO	Open

0	1	1	1	14	17
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL

08

08 Detailed findings

PoC note: fork tests run at BSC block 128,976,460 (21 October 2026) against the live bytecode, with a confirmation rerun of the full suite. No live mainnet transaction was made. All 62 tests pass. The H-01 PoC uses vm.etch to simulate EIP-7702 re-delegation, since the engagement cannot sign as the deployer. Full tests are provided in the engagement materials.

SMC AUDITS

SMC-H-01 HIGH Open

Marketing fee receiver can halt taxed sells via EIP-7702 and .transfer()

CATEGORY

Privilege and centralization risk; denial of service and gas griefing

LOCATION

swapBack() marketing payment (.transfer()), shouldSwapBack(), setFeeReceivers(address), setSwapBackSettings(bool,uint256)

DESCRIPTION

When a non-exempt transfer that is not a buy finds at least swapThreshold (50e18 raw) in the token, _transferFrom runs swapBack before moving the sender's tokens. After the router swap, the marketing share of BNB is paid with `payable(marketingFeeReceiver).transfer(amountBNBMarketing)`. Solidity .transfer forwards 2,300 gas and reverts the caller on failure. Since BSC's Pascal hard fork, an EOA can attach contract code with one EIP-7702 authorization. A delegate whose receive or fallback reverts, or one that burns more than 2,300 gas (for example a single SSTORE), makes the marketing payment fail, swapBack reverts, and the sell reverts. Buys (msg.sender == pair) skip swapBack and keep working, so inventory can refill and every later taxed sell hits the same wall. setSwapBackSettings requires _enabled == true, so the trigger cannot be switched off. setFeeReceivers only checks !_isContract at the moment of the call; a clean EOA can be set and delegated later. Owner is 0xdEaD; only the permanently authorized deployer can change the receiver or raise the threshold.

IMPACT

Holders cannot sell into the only liquid pool while buyers can still buy, the honeypot pattern. Wallet-to-wallet transfers that trigger swapBack also revert. Fee-exempt wallets still pay through swapBack when they are the sender of a threshold-hitting transfer (the payment is independent of the sender's exemption). Only the deployer key can arm (point the receiver at a wallet they control, or re-delegate the current receiver) or lift the halt. The switch is invisible to scanners that treat owner() == 0xdEaD as no admin risk. Rated High: a total sell block under conditions the project controls, and no outsider recovery after renounce. Not Critical: it is not armed as a reverting or gas-burning payment target in the PoC baseline without etching, and there is no direct theft of balances.

PROOF OF CONCEPT

On a fork of BSC at block 128,976,460, vm.etch writes the runtime code a 7702 delegation would expose. Suite poc/test/C02_SellHalt.t.sol (9/9) and P3_LineByLine.t.sol::test_7702_isContractSnapshotOnly:

- Baseline: with inventory at or above threshold, sells trigger swapBack and succeed, marketing BNB increases.
- Etch a reverting receive or a gas-burning receive on the marketing receiver: router sells revert, direct transfers that hit swapBack revert, buys still succeed, and a fresh buyer is then trapped.
- setFeeReceivers(freshEOA) passes the isContract check; later vm.etch on that EOA reproduces the halt.

- Halt persists after a 365-day warp. Outsiders cannot setFeeReceivers, setSwapBackSettings or authorize. Only the deployer restores a clean receiver or a threshold of 1e30.
- Live trigger proximity: the contract held ~47.2e18 against threshold 50e18 at the fork, so one modest buy crosses it.

RECOMMENDATION

Live contract: immutable. The deployer should point marketingFeeReceiver at a cold EOA that will never carry 7702 code, keep that key offline, and treat it as an admin key. Holders and listing sites should monitor eth_getCode on the current receiver. Future versions: pay receivers with a pull pattern or a gas-limited call whose failure is tolerated, never put unbounded or stipend-limited failure inside the user transfer path, and keep receivers on a timelocked multisig.

SMC AUDITS

SMC-M-01 MEDIUM Open

Cosmetic renounce leaves the deployer permanently authorized

CATEGORY

Privilege and centralization risk

LOCATION

Auth (authorizations, unauthorize, transferOwnership / renounce path), all authorized setters

DESCRIPTION

At construction the deployer is owner and authorizations[deployer] = true. Moving ownership to 0xdEaD does not clear the bitmap, and unauthorize is onlyOwner, so the deployer cannot remove their own authorization and nobody else can either. The deployer retains live control of fees up to the 25% cap, the marketing receiver, fee and dividend exemptions, Zeus buyback and the sell-fee multiplier, auto-buyback, distributor gas, target liquidity and the swap threshold. onlyOwner paths (authorize, transferOwnership, setDistributionCriteria) are dead for everyone.

IMPACT

Public posture is renounced, but fee and buyback policy remain under one EOA. That enables SMC-H-01 (receiver control) and allows a 25% tax, selective exemptions and spending of accumulated buyback BNB. Caps prevent mint, blacklist and 100% tax, so this is not a honeypot by itself. Rated Medium and kept separate from H-01: the Auth surface is independently material even if the payment pattern were fixed.

PROOF OF CONCEPT

poc/test/C01_Authorized.t.sol (6/6) and P3_LineByLine.t.sol::test_auth_transferOwnership_leavesOldAuth: isOwner(DEAD), isAuthorized(deployer), unauthorize(deployer) reverts !OWNER for deployer and outsider, every authorized setter succeeds for the deployer including setFees to 2500/10000 and triggerZeusBuyback, and outsiders revert !AUTHORIZED. Confirmed against live state: isOwner(0xdEaD) is true and isAuthorized(deployer) is true, while an unauthorized address returns false.

RECOMMENDATION

Live: disclose that Auth remains with the deployer, and move operational keys to a multisig if the project continues to use Zeus and fee controls. Future versions: clear authorizations[msg.sender] on renounce, or use Ownable2Step without a parallel bitmap.

SMC AUDITS

SMC-L-01 LOW Open

ERC-20 approve race condition (SWC-114)

CATEGORY

Approvals and allowance handling

LOCATION

approve(address,uint256), approveMax(address)

DESCRIPTION

approve overwrites the allowance in one shot. There are no increaseAllowance / decreaseAllowance helpers on YUKAN (approveMax sets allowance to _totalSupply). A spender front-running an allowance change can use the prior allowance before it is replaced.

IMPACT

Standard ERC-20 race. Impact is limited to users who change non-zero allowances in place. Rated Low (house standard).

PROOF OF CONCEPT

poc/test/P2_Adversarial.t.sol: allowance moves 1000 to 500 in one call; approveMax equals totalSupply() (1e24).

RECOMMENDATION

Users should set allowance to 0 before a new non-zero value, or use permit-style flows where available. Future versions: add increase and decrease helpers.

SMC-I-01 INFO Open

Anyone can trigger swapBack; router calls use zero slippage

CATEGORY

Front-running and MEV exposure

DESCRIPTION

Any transfer (including a zero-value transfer) from a non-pair sender can run swapBack once inventory is at or above threshold. Router swaps and liquidity adds use amountOutMin = 0.

IMPACT

MEV can sandwich the swap; at the live threshold the round-trip is dominated by the 4% tax (see SMC-I-02). Zero slippage is template practice.

RECOMMENDATION

Future versions: permissioned or time-bounded swap triggers, non-zero slippage bounds or a private relay.

SMC AUDITS

SMC-I-02 INFO Open

SwapBack sandwich is unprofitable at the live threshold

CATEGORY

Front-running and MEV exposure

DESCRIPTION

At fork state the threshold is about 0.14% of the pair token balance. A 2 BNB buy, victim swapBack, sell sandwich loses to the 4% tax.

IMPACT

No practical extraction from ordinary swapBack size today.

RECOMMENDATION

None required at current size; revisit if the threshold is raised materially.

SMC-I-03 INFO Open

Zeus buyback sandwich can profit at large authorized size

CATEGORY

Front-running and MEV exposure

DESCRIPTION

Live contract BNB (~0.076 to ~0.089 across measurements) is too small for a profitable sandwich. Funding the contract with ~1 BNB and calling Zeus lets a sandwich profit from buyback inefficiency. Requires an authorized trigger.

IMPACT

Value comes from reduced burn efficiency, not from pulling holder balances. Authorized-gated.

RECOMMENDATION

Keep Zeus sizes modest relative to pool depth; prefer private submission for large buybacks.

SMC AUDITS

SMC-I-04 INFO Open

DTG reward token takes 9% fee-on-transfer on claims

CATEGORY

Token and supply logic; external dependency

DESCRIPTION

DTG is renounced with fixed 3%+3%+3% fees and no blacklist. The distributor is not excluded. Claims mark the full unpaid amount paid while the holder receives about 91% and the distributor inventory drops by about 100% of unpaid (sender-side debit). Deposit uses a balance-delta credit and is FoT-safe on receive.

IMPACT

Holders receive less DTG than the accounting credit. No YUKAN balance theft.

RECOMMENDATION

Document the haircut for holders. Future versions: exclude the distributor on the reward token, or credit the received delta on claim.

SMC-I-05 INFO Open

Shareholder dust-grief raises gas without a durable sell freeze

CATEGORY

Denial of service and gas griefing

DESCRIPTION

Dust-seeding new shareholders increases work on transfers. Under pressure some dust transfers reverted in PoC, but a fresh buyer could still buy and sell. distributorGas is capped at 500k, far under BSC's 16,777,216 per-transaction limit.

IMPACT

Grief cost to the attacker; no persistent outsider sell halt.

RECOMMENDATION

Future versions: minimum share to enter the rotation; stricter deposit gates.

SMC AUDITS

SMC-I-06 INFO Open

Transfers to the zero address are allowed; supply is not reduced

CATEGORY

Token and supply logic

DESCRIPTION

Transfers to address(0) succeed (fee applied); totalSupply stays 1e24. Sends to 0xdEaD correctly reduce getCirculatingSupply.

IMPACT

Cosmetic supply confusion for explorers that treat zero-address balance as burned.

RECOMMENDATION

Future versions: revert on zero recipient or route burns through an explicit burn that drops totalSupply.

SMC-I-07 INFO Open

_totalSupply infinite-allowance sentinel never decrements

CATEGORY

Approvals and allowance handling

DESCRIPTION

When allowance equals _totalSupply, transferFrom does not decrement it (intentional max-approve pattern).

IMPACT

Spender retains unlimited allowance until explicitly cleared.

RECOMMENDATION

Users should treat approveMax as permanent until approve(0).

SMC-I-08 INFO Open

Emptying the pair would brick sells at roughly the pool BNB cost

CATEGORY

Denial of service and gas griefing

DESCRIPTION

Draining WBNB reserves (~15 to 16 BNB at review) would prevent meaningful sells. Cost approximates the reserve.

IMPACT

Irrational grief; same class as other pool-drain Infos.

RECOMMENDATION

None beyond ordinary liquidity monitoring.

SMC AUDITS

SMC-I-09 INFO Open

Buyback-fee BNB accumulates in the token until Zeus or auto-buyback

CATEGORY

Privilege and centralization risk

DESCRIPTION

When fees route to buyback, swapped BNB stays on the token contract. Only authorized Zeus or auto-buyback spends it.

IMPACT

Idle BNB is not a permissionless drain; it concentrates spend authority with the deployer (SMC-M-01).

RECOMMENDATION

Disclose residual BNB policy; future versions auto-buyback on a fixed schedule.

SMC-I-10 INFO Open

buyBacker mapping does not gate Zeus; authorized does

CATEGORY

Access control, signer and owner checks

DESCRIPTION

buyBacker[addr] can be toggled, but Zeus requires authorized. Clearing the deployer's buyBacker flag does not remove Zeus.

IMPACT

Misleading ACL surface; no extra privilege for strangers.

RECOMMENDATION

Future versions: remove the dead mapping or wire it into Zeus.

SMC-I-11 INFO Open

setIsFeeExempt is one-way

CATEGORY

Privilege and centralization risk

DESCRIPTION

The setter writes isFeeExempt[account] = true only; there is no clear path.

IMPACT

Exemptions granted by the deployer are permanent for that address.

RECOMMENDATION

Future versions: add a boolean parameter to set or clear.

SMC AUDITS

SMC-I-12 INFO Open

setSwapBackSettings cannot disable swapBack

CATEGORY

Denial of service and gas griefing

DESCRIPTION

The function requires _enabled and _amount at least totalSupply/100,000, so swapEnabled cannot be set false. This permanently keeps the SMC-H-01 trigger path available whenever inventory is high.

IMPACT

No emergency off switch for swapBack after a hostile receiver delegation.

RECOMMENDATION

Future versions: allow disabling swapBack under timelock, or tolerate failed marketing payments.

SMC-I-13 INFO Open

Circulating supply of zero bricks swapBack sells

CATEGORY

Arithmetic, overflow, and precision

DESCRIPTION

getCirculatingSupply is totalSupply minus balance(DEAD) minus balance(ZERO). If circulating is forced to zero, liquidity-backing math reverts and swapBack fails, so sells that trigger it revert. Buys still work. Reaching this state on a live token requires essentially all supply at DEAD or ZERO.

IMPACT

Extreme and irrational; not a practical outsider grief.

RECOMMENDATION

Future versions: guard getLiquidityBacking when circulating is zero and skip LP math instead of reverting.

SMC AUDITS

SMC-I-14 INFO Open

Over-liquified state skips auto-liquidity (by design)

CATEGORY

Fee, tax, and reflection mechanics

DESCRIPTION

When backing is at or above target, the liquidity fee component is treated as zero for that swapBack and BNB is not added as LP. Configurable via setTargetLiquidity.

IMPACT

By design; marketing, reflection and buyback shares still process.

RECOMMENDATION

Document the target for holders; no code change required.

09

09 Remediation status

After the project addresses the findings, SMC Audits re-audits the changes and records the outcome here. The reviewed contract is immutable (not a proxy) and the owner slot is 0xdEaD, so on-chain code changes are not possible. Operational mitigation for SMC-H-01 and SMC-M-01 sits with the permanently authorized deployer (receiver hygiene, key custody, disclosure). The rest is advisory for holders, integrators and any future redeployment.

ID	SEVERITY	STATUS	VERIFIED FIX
SMC-H-01	HIGH	Open	None (immutable). Deployer can point the fee receiver at a cold undelegated EOA.
SMC-M-01	MEDIUM	Open	None (immutable). Disclose Auth; prefer multisig for remaining powers.
SMC-L-01	LOW	Open	None (immutable). Users set allowance to 0 before replacement.
SMC-I-01	INFO	Open	None. Applies to future versions.
SMC-I-02	INFO	Open	None. Measured unprofitable at live size.
SMC-I-03	INFO	Open	None. Authorized-gated; size discipline.
SMC-I-04	INFO	Open	None. Reward-token dependency.

SMC-I-05	INFO	Open	None. No durable freeze proven.
SMC-I-06	INFO	Open	None. Applies to future versions.
SMC-I-07	INFO	Open	None. Document approveMax behaviour.
SMC-I-08	INFO	Open	None. Liquidity monitoring.
SMC-I-09	INFO	Open	None. Disclose residual BNB policy.
SMC-I-10	INFO	Open	None. Applies to future versions.
SMC-I-11	INFO	Open	None. Applies to future versions.
SMC-I-12	INFO	Open	None. Applies to future versions.
SMC-I-13	INFO	Open	None. Extreme condition.
SMC-I-14	INFO	Open	None. By design.

Open items for completeness: (1) The H-01 evidence is a fork simulation, marketing-receiver code was written with vm.etch to model EIP-7702 re-delegation, and no deployer key was used. (2) Balances, reserves and BNB figures are at block 128,976,460 (21 October 2026, Africa/Lagos); active wallets change. (3) The candidate fee-clear divide-by-zero (C-04) was closed with no finding across five PoCs. (4) solc 0.8.4 known-bug review: SafeMath wrappers are redundant under 0.8 checked arithmetic, and no applicable compiler bug was found for this bytecode path.

10

10 Conclusion

At the reviewed address, Yukan is a PinkSale buybackBaby fee token with DTG holder rewards, a 4% pair tax, automatic swap-back, Zeus buyback and a Safemoon-style Auth module whose owner slot reads as renounced while the deployer stays permanently authorized.

The review found one High, one Medium, one Low and fourteen Informational items. The High is the marketing-receiver sell halt under EIP-7702 when payment uses .transfer(). The Medium is the cosmetic renounce. No outsider freeze or drain was proven, LP is almost entirely burned, and the approve race is the house Low.

Readers should treat the deployer key and the current marketing fee receiver as admin surfaces despite owner() == 0xdEaD, monitor eth_getCode on the receiver for a 0xef0100... prefix, and read

DTG's 9% claim haircut before relying on reflected rewards.

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