



tapehack

ON-CHAIN SECURITY AUDIT

INTERIM SECURITY AUDIT REPORT

TapeUp

Smart Contracts and Web Security

Report ID	TH-2026-002
Report version	V1.0.1
Subject	Identified source and historical records
Evidence period	2026-10-12 / 2026-10-14
Report date	2026-10-15
Companion	Remediation Spec for AI Vibe Coding

Conclusions are limited to the identified source and evidence dates.
Modified versions fall outside this report.

Reading Guide

REPORT

Security Audit Report · PDF
Conclusions, risks and decisions in concise lists.

COMPANION

Remediation Spec · Markdown
Itemized changes, invariants and acceptance cases for implementation and AI coding tools.

Interim assessment: This report consolidates identified source and records from 2026-10-12 to 2026-10-14; it does not certify deployment on 2026-10-15. Modified versions fall outside scope. Chinese controls if translations differ.

Contents

01	Conclusion	3
02	High and Medium Risks	4
03	Issue Register	5
04	Who Can Move Assets	6
05	Verification of Related Claims	7
06	User Notices	7
07	Conditions Requiring Reassessment	8
08	Scope and Limitations	8
09	Positive Measures	9
10	Disclaimer	9

01 Conclusion

Project-wide clearance is not supported.

Project	TapeUp / BNB Chain
Source	Source delivered 2026-10-12 and identified historical source
Report ID	TH-2026-002 / V1.0.1
Evidence boundary	2026-10-12 / 2026-10-14

C01

High · privileged
conditional risk

C02

Medium · supplied-
source vulnerability

Deployment

Source correspondence
unknown

Web

No confirmed
vulnerability; limited
scope

- Overall: the evidence does not support project-wide security clearance or final release approval.
- Contracts: C01 is a High privileged conditional risk; C02 is a Medium supplied-source vulnerability. Neither establishes an observed attack or the same flaw in live code.
- Web: no vulnerability was confirmed in the existing public-page and interface records. Incomplete coverage cannot exclude High or Medium issues elsewhere in the application.
- Source and deployment: the two pool sources delivered on 2026-10-12 were not tied to the observed running or queued implementations. Findings cannot be transferred to unknown code.
- This report consolidates records from 2026-10-12 to 2026-10-14. No new target requests, signatures or transactions were made on 2026-10-15.

Priorities and Classification

- Resolve first: unknown final implementation identity, possible weakening of the upgrade exit window, and reward weight retained after NFT exit.
- Then address: old-token liabilities, cross-pool exit dependencies, numeric/address configuration, deployment permissions and storage migration assurance.
- The register retains vulnerabilities, conditional risks, hardening, accepted design observations, unsupported hypotheses and unknowns. Its row count is not a vulnerability count.

02 High and Medium Risks

C01 · Concentrated upgrade authority and an inadequate exit window

High - privileged conditional risk

- **Cause** Both supplied pools authorize UUPS upgrades through owner, with no enforced waiting period in the supplied source. Historical state showed the same no-code owner address for both pools. A later fixed-block record showed a 48-hour running delay and a queued implementation returning 2 seconds.
- **Impact** A malicious or compromised authorized controller can replace pool logic and move assets held by the pools, and may use approvals that remain valid. No key compromise, malicious upgrade or theft was established.
- **Boundary** Requires control of the authorized owner or governance path. The queued 2-second value was not proved active. No source correspondence or execution state was established for 2026-10-15.
- **Response** Fix the final build identity first. Put both pools behind a multisig-controlled timelock with at least 172800 seconds of minimum delay, including critical configuration and delay changes. Cancel or replace an unsafe queued change through an authorized process. A planned ownership migration is not a completed control.

C02 · Ineligible principal can keep earning after NFT withdrawal

Medium - supplied-source vulnerability

- **Cause** NFT-only exit functions omit BEM reconciliation; ordinary NFT exit catches a failed callback. Existing evidence also records a gas-sensitive callback-failure path. BEM reward accounting can retain stake that the user no longer supports with NFTs.
- **Impact** A user can rotate one NFT among funded addresses and retain excess reward weight. The recorded example gave three 100-BEM positions a 75% share against one honest 100-BEM position. This is a reward-dilution example, not an observed on-chain loss or principal theft.
- **Boundary** Requires the supplied code to be used, valid NFT access, actual BEM principal at each address, later keeper distribution and a period without effective reconciliation. The observed deployed implementation was not proved to have the new exit functions.
- **Response** Make reward eligibility invalidation reliable across every NFT exit, transfer and cap reduction. Do not restore the old exit lock by requiring a fallible external refund on every exit. Do not rely only on public reconcile or an off-chain keeper sweep.

Coupled fixes: C02 and C04 must preserve both safe exit and valid reward weight. Permissive exit alone or mandatory external refunds alone is insufficient.

03 Issue Register

Contract Matters

ID	Matter	Nature and status	Required action
C01	Concentrated upgrade authority and an inadequate exit window	● High - privileged conditional risk	Use a multisig-controlled timelock; preserve the exit window
C02	Ineligible principal can keep earning after NFT withdrawal	● Medium - supplied-source vulnerability	Fix safe exits and reward eligibility together
C03	Unpaid reward debt can be redenominated after exit	● Low - residual risk	Segregate debt by token or block changes while debt remains
C04	BEM principal exit still depends on the other pool	● Low - conditional risk	Preserve safe principal exit when dependencies fail
C05	Source is not tied to running or queued implementations	● Reported Low - deployment assurance gap	Provide final implementation sources and build correspondence
C06	Numeric configuration lacks safe business bounds	● Low - configuration risk	Bound parameters without blocking safe exit
C07	A no-code token target can appear to transfer successfully	● Informational - configuration gap	Validate token code; retain debt on payment failure
C08	The BEM pool address lacks code validation	● Informational - configuration gap	Validate pool interfaces and retain safe exits
C09	One-step ownership transfer and renunciation risks	● Informational - governance hardening	Require acceptance; prevent accidental renunciation
C10	Keeper permissions default to unset after upgrade	● Informational - deployment prerequisite	Configure required permissions atomically with upgrade
C11	Shape-based NFT eligibility needs a product decision	● Low candidate - specification unresolved	Define netlist policy and existing-exception treatment
C12	Large NFT batches can exceed a transaction budget	● Informational - availability	Support bounded batches and per-token exits
C13	Rewards use a point-in-time stake snapshot	● Design accepted in the existing conclusion	Disclose the snapshot rule; reassess economic changes
C14	Rounding dust remains in the pools	● Precision observation accepted in the existing conclusion	Preserve conservation and define any changed dust rule
C15	Distribution is restricted; simple annualization needs disclosure	● Permission path restricted - display observation	Retain keeper restrictions and label the metric accurately
C16	Historical storage and migration assurance is incomplete	● Partial assurance - more evidence needed	Provide implementation history, layouts and migration inputs
C17	The old missing-NFT-list hypothesis was not supported	● Not substantiated - not a confirmed vulnerability	Retain NFT inventory consistency regression cases
C18	The old nonstandard-BEM-behavior hypothesis was not established	● Not substantiated - not a confirmed vulnerability	Retain received-amount accounting; reassess token changes

See section 02 for C01/C02. Locations, constraints and acceptance cases for every item are in section 4 of the companion spec.

03 Issue Register (continued)

Web Matters

ID	Matter	Nature and status	Required action
W01	Sampled earn pages block framing	● Positive change - limited scope	Retain protection and cover sensitive routes
W02	Legacy TLS remains negotiable	● Hardening gap	Disable TLS 1.0/1.1; verify modern clients
W03	HSTS is missing; HTTP redirects remain unknown	● Hardening gap / unknown	Verify HTTPS, HSTS and hostname scope
W04	RPC controls exist; full resource boundaries are unknown	● Positive change / unknown	Document method, count, byte and execution budgets
W05	Two specific RPC methods were denied	● Positive change - limited scope	Verify policy per method and upstream
W06	Public RPC distinguishes browser origins	● Positive control - not proof of authentication	Separate origin policy, authentication and quotas
W07	A user-selected RPC can mislead balance display	● Conditional risk	Expose trust and validate chain and stale data
W08	Controlled wallet samples worked; real flows remain incomplete	● Observation / incomplete validation	Validate real wallets, signing and session lifecycle
W09	RPC error handling has compatibility issues	● Compatibility	Normalize error classes and request-ID correlation
W10	SSE evidence covers only short initial events	● Observation / unknown resource bounds	Validate reconnect, replay, cleanup and limits
W11	Full application, private APIs and operations remain incomplete	● Assurance gap / unknown	Provide source, role-specific objects and configuration

04 Who Can Move Assets

Role	Asset and authority boundary
Upgrade controller	Can replace pool logic. Pooled NFTs/BEM and still-valid approvals carry governance trust risk. Key compromise or malicious transfer was not established.
Keeper	Distributes rewards in the supplied source; this is not general principal-withdrawal authority. Final permissions and initialization need verification.
Ordinary user	Operates their own position under the rules. C02 requires real principal and eligible NFTs; it does not create assets without funding.
External component controller	Token, NFT and upgradeable dependencies can change semantics. Their complete security and authority are outside the two-pool source assurance.

05 Verification of Related Claims

These are paraphrases of relevant claims, not verbatim quotations or all statements attributed to the project.

Related claim	Assessment
No High or Medium issues	Unsupported project-wide. C01/C02 concern contracts; no confirmed Web vulnerability does not cover contracts.
Fixed / deployed	Requires exact source hashes, a deployment block and full acceptance evidence. The current correspondence is insufficient.
The 2-second delay is active	Not established. The key record showed a 48-hour running delay and a 2-second queued value. Eligibility is not execution.
Reward-token switching is fully fixed	Unsupported. Active-stake switching was restricted, but C03 retains the exited-user liability path.
Unlimited RPC / recovery in 15 seconds	Neither is supported. Batch rejection and 429 exist; a successful recovery sample was 66.173 seconds after the first 429. The exact window is unknown.
Framing, origins and wallet flows passed	Limited pages or controlled samples only; not all routes, authentication, real wallets or private-object access.

06 User Notices

- Until deployment identity and governance state are verified, users should understand that upgrade control can change asset-handling logic.
- Displayed balances, annualized rates and custom-RPC reads are not proof of receipt, final transaction success or guaranteed return.
- Rewards use a distribution-time snapshot, without holding-time weighting, and require eligible funded positions and keeper distribution.
- Missing headers, public module names, HTTP 200 or an old framing screenshot alone do not establish theft, unauthorized access or injection.

07 Conditions Requiring Reassessment

- Changes to proxy, implementation, queue, owner, timelock threshold/delay, keeper or critical parameters.
- Changes to pool source, compiler inputs, storage, migration, reward token, NFT admission or reward economics.
- Changes to ingress, RPC upstream/policy, custom nodes, wallet connection, frontend/backend/worker, dependencies or build.
- New private objects, account roles or real-fund operations; changed prerequisites or new impact evidence.

08 Scope and Limitations

- Contracts: existing conclusions for TapeUpBEMPool.sol and TapeUpCircuitPool.sol, plus specified historical identity, authority and accounting records.
- Web: sampled public pages at tapeup.io and tapeup.org, and bounded existing records for rpc.tapeup.io and version.tapeup.io.
- Excluded assurance: complete NFT/token/external-protocol audits, unknown implementation source, all private APIs, and real-wallet signing or funds transactions.

Key Governance Snapshot (not live state on 2026-10-15)

- BNB Chain, chain ID 56; block 127368860, 2026-10-13 16:13:53 UTC+08:00.
- The running delay was 172800 seconds; both queued implementations returned 2 seconds.
- Earliest queue execution: Circuit 2026-10-15 10:03:33; BEM 10:04:27 (UTC+08:00). No execution on the report date was established.

BEM pool proxy	0x44040495ac4d64e9deaa6d0d23e695cf9fda8c2b
Circuit pool proxy	0xf5566d1e70d7668cb17956db213907ddc9dc2d90

Source Identity (SHA-256; identifies reviewed material only)

Historical reviewed source TapeUpBEMPool.sol 7601fc169dc048961b536515e0231f432686f34cf44b6fe1c9faa04cf8aeb9d1	Historical reviewed source TapeUpCircuitPool.sol 7054b2121bc470be0d87a51bda7aafc810aaf5a8f7b627eae784548eaa0369a4
Source delivered 2026-10-12 TapeUpBEMPool.sol a6b710d1846708bfc0d936e194fcb8b261ac538cd152c754004bf392a4511f37	Source delivered 2026-10-12 TapeUpCircuitPool.sol bf37b27844b852063cc0fc4f7842004bad070ed895e6e4972dc9a2f36da08fad

08 Scope and Limitations (continued)

Remaining Conditions

Category	Limits and required conditions
Real funds	Funding applies only to separately authorized, optional mainnet trade cases. Signing and login need no funds, but require real entry points, rules and authority. Actual fund impact remains unverified.
Dedicated environment	Resource limits, faults, replay and recovery need an approved isolated environment and backend visibility; small samples cannot establish the boundaries.
Internal implementation	Final source, locks, deployment configuration, backend, logging/alerts and complete migration history remain unavailable.
Multiple roles / permissions	Distinct approved roles and separate business objects are needed for private-object authorization, revocation and session validation.

09 Positive Measures

- The supplied source restricts distribution to keepers and adds exits decoupled from reward failure; reward eligibility still needs repair alongside safe exit.
- Old fields were preserved between the provided source layouts. The specified historical NFT inventory and accounting did not support the old missing-list hypothesis.
- Specified earn pages showed effective framing protection. Bounded method rejection, batch rejection, 429 and public Origin distinctions were recorded.
- Standard account switching, controlled connection restoration and disconnect samples behaved correctly. All positive observations retain their time and scenario limits.

10 Disclaimer

- This interim report gives limited opinions on the identified source and historical records. It is not current-deployment certification, a no-vulnerability guarantee, investment advice or release approval.
- No observed attack does not mean no attack exists. Untested, blocked or undocumented areas cannot be marked passed.
- Modified versions fall outside this report. Closure requires the final corresponding deployment to reject the original impact while legitimate controls work.
- This report and its companion spec share TH-2026-002 / V1.0.1. Chinese controls if the translations differ.

