



tapehack

ON-CHAIN SECURITY AUDIT

阶段性安全审计报告

# TapeUp

智能合约与 Web 安全审计

|      |                          |
|------|--------------------------|
| 报告编号 | TH-2026-002              |
| 报告版本 | V1.0.1                   |
| 审计对象 | 指定源码及历史记录                |
| 证据时段 | 2026-10-12 / 2026-10-14  |
| 报告日期 | 2026-10-15               |
| 配套文件 | 修复规格书 For AI Vibe Coding |

结论适用于标识的源码与证据时点。  
修改后的版本不在本报告范围内。

# 阅读指引

本报告

安全审计报告 · PDF

结论、风险和需要做的决定，按清单列出。

配套文件

修复规格书 · Markdown

逐项修改边界、不变量和验收用例，供实施及 AI 编程工具使用。

阶段性审计说明：本报告汇总指定源码与2026-10-12至2026-10-14历史记录；不是2026-10-15部署认证。任何修改版本均超出本报告范围，中英文差异以中文为准。

# 目录

|    |           |   |
|----|-----------|---|
| 01 | 结论        | 3 |
| 02 | 高危与中危风险   | 4 |
| 03 | 问题总表      | 5 |
| 04 | 谁能转移资产    | 6 |
| 05 | 相关说法核对    | 7 |
| 06 | 用户须知      | 7 |
| 07 | 需要重新评估的条件 | 8 |
| 08 | 范围与限制     | 8 |
| 09 | 正面措施      | 9 |
| 10 | 免责声明      | 9 |

01 结论

尚不足以判定项目整体通过。

|      |                         |
|------|-------------------------|
| 项目   | TapeUp / BNB Chain      |
| 源码   | 2026-10-12交付源码与标识的历史源码  |
| 报告编号 | TH-2026-002 / V1.0.1    |
| 结论时点 | 2026-10-12 / 2026-10-14 |

|                                       |                                       |                                  |                                        |
|---------------------------------------|---------------------------------------|----------------------------------|----------------------------------------|
| <div>C01</div> <div>高危 · 特权条件风险</div> | <div>C02</div> <div>中危 · 送审源码漏洞</div> | <div>部署</div> <div>源码对应未确认</div> | <div>Web</div> <div>未确认漏洞 · 覆盖有限</div> |
|---------------------------------------|---------------------------------------|----------------------------------|----------------------------------------|

- 整体结论：目前不足以给出项目整体安全通过或最终上线放行结论。
- 合约：C01 为高危特权条件风险；C02 为中危送审源码漏洞。它们不等同于已发生攻击或已确认线上同类漏洞。
- Web：既有公开页面及接口记录未确认漏洞；覆盖仍不完整，不能据此排除整个应用的高危或中危问题。
- 源码与部署：2026-10-12交付的两池源码尚未对应到已观察运行或预约实现；未知实现的风险不能从送审源码直接推定。
- 本文件汇总2026-10-12至2026-10-14的已有资料；2026-10-15未新增目标请求、签名或交易。

处理优先级与分类

- 优先解除：最终实现身份不明、升级退出窗口可能被削弱、NFT退出后无资格本金仍参与分奖。
- 随后处理：旧币负债、跨池退出依赖、参数及地址配置、部署权限初始化、历史存储迁移保证。
- 分类口径：总表同时保留漏洞、条件风险、加固事项、设计观察、未获支持假设及未知；不把条目总数当作漏洞数量。

## 02 高危与中危风险

### C01 · 单一升级权及退出窗口不足

高危·特权条件风险

- **成因** 送审两池源码通过owner授权UUPS升级，未强制升级等待期。历史链上记录显示两池为同一无代码owner地址；后续指定区块记录显示运行延迟48小时、预约实现延迟2秒。
- **影响** 恶意或失陷的有权控制者可替换池逻辑，转移池内NFT、BEM及有效授权范围内的资产。无已发生盗取、恶意升级或密钥失陷证据。
- **边界** 需要控制有权owner或治理路径。2秒仅为预约实现读取值；未证明其已生效，也未核实2026-10-15的执行状态及源码对应关系。
- **怎么办** 先固定最终上线构建；两池由多签控制的时间锁管理，升级、关键参数及延迟变更均受不少于172800秒的等待约束。通过有权流程取消或替换不安全预约；迁移计划不能代替已完成控制。

### C02 · NFT退出后无资格本金仍参与分奖

中危·送审源码漏洞

- **成因** 送审源码的unstakeOnly / unstakeAllOnly跳过BEM reconcile；普通NFT退出吞掉失败回调，已有记录还存在gas敏感回调失败路径。奖励账目因此可能保留已失去NFT支持的BEM权重。
- **影响** NFT轮转多个地址后，各地址的BEM仍计入全局奖励权重，稀释合规质押者收益。已有本地示例一张攻击者NFT形成3个100 BEM仓位，与1个诚实100 BEM仓位相比取得75%奖励。影响为奖励分配，未证明本金盗取。
- **边界** 交付源码unstakeOnly/unstakeAllOnly跳过reconcile；普通unstake也吞回调失败，既有材料报告存在精确gas导致回调失败的路径。还需要攻击者提供各地址的真实BEM本金、有效NFT及后续keeper发奖；没有人及时reconcile。
- **怎么办** 修复应使所有退出/转移/调低上限路径中的有效奖励权重同步失效，且必须保留安全取回本金与NFT的能力。仅让所有退出强制外部退款会重新引入已修复退出依赖；仅公开reconcile或链下keeper补偿也不足以保证不变量。

关联修复：C02与C04必须同时满足安全退出和奖励资格约束；不能只放开退出或只强制外部退款。

### 03 问题总表

#### 合约事项

| 编号  | 事项               | 性质与状态          | 处理要求              |
|-----|------------------|----------------|-------------------|
| C01 | 单一升级权及退出窗口不足     | ● 高危·特权条件风险    | 多签控制时间锁；不得削弱退出窗口  |
| C02 | NFT退出后无资格本金仍参与分奖 | ● 中危·送审源码漏洞    | 联合修复退出与有效奖励权重     |
| C03 | 退出后旧收益负债仍可被换币    | ● 低危·残余风险      | 按币种保留负债或在旧债非零时禁换  |
| C04 | BEM本金退出仍依赖跨池接口   | ● 低危·条件风险      | 故障时保留安全本金退出       |
| C05 | 送审源码与运行/预约实现不对应  | ● 低危·记录·部署保证缺口 | 取得最终实现源码和构建对应证明   |
| C06 | 数值配置缺少安全上限       | ● 低危·误配置风险     | 定义业务上限，保障极值退出     |
| C07 | 无代码代币地址可能被判转账成功  | ● 提示·配置缺口      | 验证代币代码；失败不清债      |
| C08 | BEM池地址缺少代码校验     | ● 提示·配置缺口      | 校验池接口并保留容错退出      |
| C09 | 所有权单步转移及放弃权限风险   | ● 提示·治理加固      | 两步接收，阻止误放弃        |
| C10 | 升级后keeper默认未配置   | ● 提示·部署条件      | 升级与必要权限配置原子完成     |
| C11 | 同形状NFT准入规则尚待确认   | ● 低危·候选·待规则    | 确认网表规则及历史例外处理     |
| C12 | 大批NFT操作的单笔可用性    | ● 提示·可用性       | 支持分批及逐token退出     |
| C13 | 即时快照式奖励分配        | ● 既有结论接受的设计    | 披露快照规则；改变经济模型需复核  |
| C14 | 舍入余数留存           | ● 既有结论接受的精度事项  | 保留守恒；变更时明确余数规则    |
| C15 | 发奖权限已收紧，简单年化仍需说明 | ● 权限路径已限制·指标提示 | 保留keeper限制，标注指标含义 |
| C16 | 历史布局与迁移保证不完整     | ● 部分核对·待资料     | 补全历史实现、布局和迁移输入    |
| C17 | NFT列表遗失旧假设未获支持   | ● 未获支持·不计漏洞    | 保留清单一致性回归         |
| C18 | BEM非标准行为旧假设未获证实  | ● 未获支持·不计漏洞    | 保持实收记账，变更代币须复核    |

C01/C02详见第02节；全部事项的位置、修改边界和验收条件见《修复规格书》第4节。

### 03 问题总表（续）

#### Web事项

| 编号  | 事项                 | 性质与状态         | 处理要求                 |
|-----|--------------------|---------------|----------------------|
| W01 | 所测收益页已阻止嵌入         | ● 正面变化·范围有限   | 保留防护并覆盖敏感路由          |
| W02 | 旧版TLS仍可协商          | ● 加固缺口        | 禁用TLS1.0/1.1，验证现代客户端 |
| W03 | HSTS缺口，HTTP跳转未知    | ● 加固缺口 / 未知   | 核实HTTPS、HSTS与域名范围    |
| W04 | RPC有限防护存在，完整阈值未知   | ● 正面变化 / 未知   | 取得方法、条数、字节及执行预算      |
| W05 | 两个具体RPC方法被拒        | ● 正面变化·范围有限   | 核对逐方法、逐上游策略          |
| W06 | 公开RPC存在Origin区分    | ● 正面措施·非认证证明  | 将来源策略与认证、配额分开        |
| W07 | 用户自选节点可误导余额显示      | ● 条件性风险       | 明确可信来源，校验网络及陈旧读数     |
| W08 | 受控钱包连接样本正常，真实流程未全验 | ● 观察 / 未完整验证  | 补真实钱包、签名及会话验证        |
| W09 | RPC错误格式仍有兼容性事项     | ● 兼容性         | 统一错误类别和请求ID关联        |
| W10 | SSE只覆盖短连接首事件       | ● 观察 / 资源边界未知 | 验证重连、重放、释放与限额        |
| W11 | 完整应用、私密接口和运维覆盖仍缺   | ● 保证缺口 / 未知   | 补源码、权限对象及部署配置        |

### 04 谁能转移资产

| 角色      | 资产与权限边界                                         |
|---------|-------------------------------------------------|
| 升级控制者   | 可替换池逻辑；池内NFT、BEM及仍有效的授权资产存在治理信任风险。未证明密钥失陷或恶意转移。 |
| keeper  | 在送审源码中负责发奖；不是通用本金提款授权。最终部署权限及初始化仍须核实。           |
| 普通用户    | 可按规则操作自己的仓位；C02需要真实本金和有效NFT，不是无本金复制资产。          |
| 外部组件控制方 | 代币、NFT及其可升级依赖可能改变语义；不在两池完整源码保证内，需单独确认权限。        |

## 05 相关说法核对

以下为相关说法的概括转述，非逐字引述，也不全部归属于项目方。

| 相关说法            | 核对结果                                              |
|-----------------|---------------------------------------------------|
| 项目没有高危或中危       | 不成立为整体结论。合约存在C01/C02，Web未确认漏洞不覆盖合约。               |
| 已修复 / 已部署       | 只接受与具体源码哈希、部署区块和完整验收对应的说法；目前对应关系不足。               |
| 2秒延迟已经生效        | 未证实。关键记录中运行值48小时、预约实现值2秒；到期不代表执行。                 |
| 旧奖励代币问题已全部修复    | 不成立。活跃质押路径收紧，但退出后旧负债路径C03仍需处理。                    |
| RPC无限制 / 15秒恢复  | 均无充分依据。已见batch拒绝与429；恢复成功样本距首个429为66.173秒，精确窗口未知。 |
| 防嵌入、来源及钱包全流程已通过 | 只成立于限定页面或受控样本；不证明全部路由、认证、真实钱包和私密对象安全。             |

## 06 用户须知

- 在部署身份及治理状态核实前，用户应理解升级控制者可改变资产处理逻辑。
- 展示余额、年化收益或自选RPC读数不是资产到账、交易最终成功或保证收益证明。
- 奖励使用发奖时快照，非持有时间加权；需实际有效资产并依赖keeper发奖。
- 缺失响应头、公开模块名称、HTTP 200或旧嵌入截图本身不证明盗币、越权或注入。

## 07 需要重新评估的条件

- 代理、实现、预约、owner、时间锁门限或延迟、keeper、关键参数发生变化。
- 两池源码、编译输入、存储布局、迁移、收益代币、NFT准入或奖励经济规则发生变化。
- 域名接入、RPC上游或策略、自选节点、钱包连接、前后端 / Worker、依赖或构建发生变化。
- 新增私密业务对象、账号角色或真实资金操作；原有条件不再满足或出现新的影响证据。

## 08 范围与限制

- 合约范围：TapeUpBEMPool.sol、TapeUpCircuitPool.sol的既有源码结论，以及指定历史链上身份、权限与账目记录。
- Web范围：tapeup.io、tapeup.org的已采样公开页面，以及rpc.tapeup.io、version.tapeup.io的限定既有记录。
- 不包含：完整NFT / 代币 / 外部协议审计、未提供实现源码的安全保证、全部私密接口、真实钱包签名与资金交易验证。

### 关键治理时点（不是2026-10-15实时状态）

- BNB Chain, chain ID 56；区块127368860，2026-10-13 16:13:53 UTC+08:00。
- 当时运行实现延迟172800秒；两份预约实现读取值均为2秒。
- 预约最早执行时点：Circuit 2026-10-15 10:03:33；BEM 10:04:27（UTC+08:00）。未取得2026-10-15已执行的证据。

|                    |                                            |
|--------------------|--------------------------------------------|
| BEM pool proxy     | 0x44040495ac4d64e9deaa6d0d23e695cf9fda8c2b |
| Circuit pool proxy | 0xf5566d1e70d7668cb17956db213907ddc9dc2d90 |

### 源码身份（SHA-256；仅标识所审资料）

历史已审源码

#### TapeUpBEMPool.sol

7601fc169dc048961b536515e0231f432686f34cf44b6fe1c9faa04cf8aeb9d1

历史已审源码

#### TapeUpCircuitPool.sol

7054b2121bc470be0d87a51bda7aafc810aaf5a8f7b627eae784548eaa0369a4

2026-10-12交付源码

#### TapeUpBEMPool.sol

a6b710d1846708bfc0d936e194fcb8b261ac538cd152c754004bf392a4511f37

2026-10-12交付源码

#### TapeUpCircuitPool.sol

bf37b27844b852063cc0fc4f7842004bad070ed895e6e4972dc9a2f36da08fad

## 08 范围与限制（续）

### 剩余条件类别

| 类别       | 限制与后续条件                                                |
|----------|--------------------------------------------------------|
| 真实资金     | 资金仅适用于另行授权的可选主网成交用例；签名和登录无需资金，仍需真实入口、规则与授权。真实资金影响尚未验证。 |
| 专用环境     | 限流资源边界、故障、回放及恢复需要获准隔离环境与可观测后端，不能从小样本推定。                |
| 内部实现     | 最终源码、锁文件、部署配置、后台、日志告警及完整迁移记录仍缺。                        |
| 多角色 / 权限 | 需具备不同合法角色及彼此隔离的业务对象，完成私密对象授权、撤权与会话验证。                  |

## 09 正面措施

- 送审源码收紧发奖为keeper权限，并提供将NFT退出与收益失败解耦的路径；仍须同时修复奖励资格。
- 已提供两份源码间的旧字段布局保持；指定历史NFT清单与账目记录未支持旧的列表遗失猜测。
- 指定收益页已出现有效防嵌入；限定RPC方法拒绝、批量拒绝、429及公开Origin区分均有记录。
- 标准账户切换、受控连接恢复和断开样本正常；正面记录均受其时间及场景限制。

## 10 免责声明

- 本阶段性报告仅对标识的源码和历史记录发表有限意见，不是当前部署安全认证、无漏洞保证、投资建议或上线批准。
- 未观察到攻击不代表攻击不存在；未覆盖、受阻或缺资料的项目不能记为通过。
- 任何修改版本均超出本报告范围；风险关闭须在对应最终部署上重新验证原影响与合法对照。
- 本报告及配套规格书同为TH-2026-002 / V1.0.1；中英文如有差异，以中文为准。