[CPK] Solutions

Security and Systems Risk Analysis

StakePoint

Smart Contract Security Audit

Retest summary

PREPARED FOR	StakePoint
PREPARED BY	CPK Solutions
ENGAGEMENT	CPK-STAKEPOINT-ENG-001
ISSUED	9 October 2026
RELEASES VERIFIED	Commits 7b74ad1 and e18ec06
DEPLOYED PROGRAM	Upgrade at slot 454670815, 8 October 2026
FOLLOWS	Security Audit report 1.0, 7 October 2026
VERSION	1.0, retest summary

Christopher Kuntz | Principal, CPK Solutions
cpk.solutions | christopher@cpk.solutions

PREPARED FOR STAKEPOINT

May be shared only in full and unaltered. See section 06 for reliance and use.

01 Retest outcome

StakePoint remediated the findings of the 7 October 2026 Security Audit report in two program releases deployed on 8 October 2026. CPK Solutions verified the deployed program against StakePoint's release record, reviewed every source change from the assessed source, and retested the deployed program in an isolated runtime.

Fifteen of the eighteen findings are resolved, including High finding SP-DEF-04 and all nine Medium findings. High finding SP-DEF-08 is mitigated: the affected legacy pool type can no longer be created or re-funded, and the remaining pools are settled on a schedule as they run to their end dates. The other two findings are an intended, disclosed behavior and an acknowledged commercial arrangement. No High or Medium finding remains unaddressed, and the retest found no regression in ordinary staking, reward, reflection, lock or vesting operations.

15	1	1	1
Resolved	Mitigated	Acknowledged	Intended behavior

Status by original severity

Original severity	Findings	Resolved	Mitigated	Acknowledged or intended
High	2	1	1	0
Medium	9	9	0	0
Low	6	5	0	1
Informational	1	0	0	1

BASIS OF STATUS

Original severities are those assigned in the 7 October 2026 report and are unchanged. Status records the outcome of remediation; residual risk describes what remains afterwards. Statuses reflect the program deployed at slot 454670815 and evidence through 9 October 2026.

02 What was verified

Releases

Release	Commit	Deployed	Executable SHA-256	Content
Remediation	7b74ad1	Slot 454638982 8 Oct 2026, 19:32 UTC	2d820fdb5fa61fb403581e642c1e068dccdcebae8f5cdb461e60e6fcd5740c2e	Remediation of SP-DEF-01 to SP-DEF-18 and the report advisories
Retest items	e18ec06	Slot 454670815 8 Oct 2026, 21:54 UTC	1eb79f89c32135da2c2b53621e0890b527b94988cdb4c819c12847d8691d875e	Closes V1 dynamic pool creation and V1 dynamic top-ups

Method

Check	What was done	Result
Deployment identity	Read the program executable from mainnet and compared it with StakePoint's release record.	Both releases match byte for byte. The second is the current deployment.
Source review	Reviewed every change from the assessed source (commit 35ccb5a) to the remediated source, including account layouts and error codes.	Every reported finding is addressed in source. Account layouts are unchanged, so existing accounts remain readable.
Runtime retest	Ran signed transactions against the deployed executable in an isolated, pinned runtime with synthetic assets: 15 regression suites and 23 fix-check suites. Existing-pool behavior was checked by applying the upgrade inside the runtime.	All 38 suites passed: 264 transactions, 242 expected to succeed and 22 expected to be rejected with a named error, and 382 state and balance checks.
Operational checks	Read-only, pool-level reads of the settlement passes and reward vault balances.	All 33 running legacy dynamic pools with open stake, and 6 of the 7 ended ones, have been settled since release. See section 04.

No testing was performed against mainnet or any live deployment. On-chain work consisted of read-only account and transaction reads.

03 Finding status

ID	Finding	Severity	Status	Retest evidence
SP-DEF-01	Native SOL transfer helper uses inconsistent custody-account semantics	Medium	Resolved	Native SOL is rejected in the transfer helper and at V1 and V2 project creation. Runtime: both creation paths reject a native mint with NativeSolUnsupported.
SP-DEF-02	Legacy reward claims change principal lock timing	Informational	Intended behavior	No change required. The behavior is intended and disclosed to users, as recorded in the report.
SP-DEF-03	Reflection claim guards exclude pending entitlement after principal exit	Medium	Resolved	The stake guard is removed from both reflection claim handlers. Runtime: a staker who has fully withdrawn claims their recorded reflections in both engines.
SP-DEF-04	Dynamic reward funding lacks an explicit prior-interval settlement boundary	High	Resolved	V2 top-ups settle accrual before the new rate applies. V1 dynamic top-ups are rejected and new V1 dynamic pools cannot be created. Runtime: both confirmed, including on an existing pool across the upgrade.
SP-DEF-05	Configured reflection mint and recorded vault can disagree	Low	Resolved	Initialization verifies the reflection account mint and owner; claims bind the supplied mint. Runtime: a mismatched mint is rejected with ReflectionMintMismatch.
SP-DEF-06	Legacy reward funding does not bind the credited vault to stored custody	Medium	Resolved	Reward funding is bound to the stored vault. Runtime: funding into any other account is rejected with UnauthorizedVault. StakePoint's project export shows every existing project stores its canonical vault.
SP-DEF-07	Legacy project creation stores a mint argument separately from account-derived identity	Low	Resolved	Mint arguments are bound to the mint accounts at V1 and V2 creation. Runtime: a mismatch is rejected with MintArgumentMismatch.
SP-DEF-08	Legacy dynamic reward pools allocate by current stake, not time-weighted participation	High	Mitigated	No new V1 dynamic pool can be created or re-funded. A crank-only settlement instruction fixes each stake's accrual on a schedule, and every running affected pool has been settled since release. Residual risk: Low. See section 04.
SP-DEF-09	Legacy reward rate changes apply to elapsed time and can block withdrawals	Medium	Resolved	Reward arithmetic saturates instead of reverting, so it can no longer block a withdrawal. The backdated-rate path is closed with SP-DEF-04.

ID	Finding	Severity	Status	Retest evidence
SP-DEF-10	Fixed-APY reward rate is quantized, systematically underpaying rewards	**Medium**	**Resolved**	Fixed APY accrues from the configured annual rate in both engines. Runtime: payouts match the configured rate, including low rates that previously accrued nothing.
SP-DEF-11	V2 fixed-APY accrual does not account for staking and reward token decimals	**Medium**	**Resolved**	V2 fixed APY requires the reward token to be the staking token, which removes the decimal mismatch by construction. Runtime confirmed; dynamic pools with a separate reward token remain supported.
SP-DEF-12	Reflection claims reset the distribution baseline without settling pending inflows	**Medium**	**Resolved**	Claims reduce the baseline by the amount sent. Runtime: reflections arriving before a claim are distributed afterwards, in both engines.
SP-DEF-13	Legacy lock extension can be set by the sole staker and binds later depositors	**Medium**	**Resolved**	Locks accept deposits only from the existing owner. Runtime: a second depositor is rejected with LockNotOwnedByDepositor; the owner can still add.
SP-DEF-14	Project administrator can hold withdrawals paused indefinitely, overriding the platform unpause	**Medium**	**Resolved**	The project pause instructions and their gates are removed, with account layouts unchanged; the separate deposit pause used by locks remains. Runtime: the instructions no longer exist and deposits are unaffected.
SP-DEF-15	Reflection per-token scaling can overflow when staked supply is very small	**Low**	**Resolved**	Overflow now saturates instead of reverting. StakePoint accepts the residual described in section 05.
SP-DEF-16	Small reflection inflows round to zero, and legacy empty-pool inflows accrue to the next staker	**Low**	**Resolved**	The baseline advances only by the amount distributed. Runtime: rounding remainders carry forward and inflows received while nothing is staked are kept for stakers.
SP-DEF-17	Project administrator can route the full platform SOL fee to a chosen referrer	**Low**	**Acknowledged**	Commercial arrangement between StakePoint and pool creators. Users pay the same fee either way and no user funds are affected. StakePoint accepts the business risk.
SP-DEF-18	Reflection pool initialization can be blocked by pre-creating the project reflection account	**Low**	**Resolved**	Account creation is idempotent and verifies mint and owner. Runtime: a pre-created account no longer blocks initialization.

04 High findings

SP-DEF-04 Dynamic reward funding: Resolved

In V2, a reward top-up now settles the global accumulator before the new rate applies, so earlier accrual keeps the rate that was in force. In the runtime retest, a top-up one hour into a pool raised the rate from 100 to 150 base units per second, and the claim paid the first hour at 100 and the second at 150.

In V1, the second release rejects top-ups to dynamic pools and prevents new V1 dynamic pools from being created. The rate of an existing V1 dynamic pool can therefore no longer be recalculated. Shortfalls are covered by direct transfer to the reward vault, which pays claims without changing the rate. This was confirmed on a pool created before the upgrade: the top-up was rejected, the rate was unchanged, and deposits, claims and withdrawals continued to work.

SP-DEF-08 Legacy dynamic allocation: Mitigated, residual risk Low

The V1 dynamic reward formula is unchanged for pools that already exist, because changing it would alter the terms of open positions. StakePoint instead closed the pool type and added controls that limit what remains:

Control	Effect
No new V1 dynamic pools	V1 pool creation accepts fixed-rate pools and locks only. The affected set is closed.
No V1 dynamic top-ups	The emission rate of an existing pool cannot change.
Scheduled settlement	A crank-only settle_stake instruction fixes each stake's accrual without moving tokens or touching lockups. Passes run per pool at a single instant, weekly while a pool runs and once after it ends, with a 24-hour minimum per stake. This limits any misallocation to the interval since the last pass.
Final settlement	A pass after a pool's end time fixes every entitlement, so later exits cannot change it.

Runtime retest of settle_stake: it is restricted to the crank authority, rejects a second settlement within 24 hours, leaves the lockup clock untouched, and after a final pass the claim pays the fixed entitlement exactly once. On mainnet, the crank authority is a separate key from the platform administrator. Since release, StakePoint has settled all 33 running V1 dynamic pools with open stake and 6 of the 7 ended ones. StakePoint states that the remaining ended pool is its own test pool with no third-party positions.

CLOSURE CONDITION

SP-DEF-08 closes when the remaining V1 dynamic pools have reached their end dates (the latest is 4 November 2027) and every stake has been settled after its pool's end. Principal is not affected: reward vaults are separate from staking vaults.

05 Additional items and existing state

Accepted and acknowledged items

Item	Record
SP-DEF-15 residual	On a pool with no or very small stake, the reflection accumulator can reach its maximum and distribution on that pool stops. The undistributed amount remains in the vault and is recoverable in a later release. StakePoint accepts this residual.
SP-DEF-17	Fee routing to a referrer is a commercial arrangement with pool creators. Users pay the same fee in every case and no user funds are affected. StakePoint accepts the business risk.
SP-DEF-02	The claim timing behavior is intended and disclosed to users. No change was required.

Additional controls in the releases

Control	Verification
Two-step platform admin transfer	Propose and accept, with the pending administrator held in a separate account. Runtime: a non-administrator cannot propose and only the proposed wallet can accept.
Rate mode validation	Unknown rate modes are rejected at pool creation in both engines. Runtime confirmed.
Minimum effective top-up	A dynamic top-up too small to raise the rate by one unit per second is rejected in V2, so funds cannot be stranded. Runtime confirmed.
Fee arithmetic	Token fee calculations use 128-bit intermediates at all five fee sites. Source review.
Extra reward claims	Claim accounts are boxed. Runtime: the ordinary extra reward claim succeeds on the deployed program.

Existing state

On one ended legacy dynamic pool, recorded rewards exceed the reward vault, an effect of SP-DEF-08 that accrued before remediation. The settlement pass fixed those figures so they cannot change further. StakePoint funded earlier claims on this pool from its own resources and has undertaken to pay the remaining recorded rewards directly to stakers who request them. All principal in the pool is withdrawable.

An administrator withdrawal instruction in an earlier program version, removed by StakePoint in March 2026 before this engagement and absent from the assessed source and the deployed program, had reduced three legacy pools' reward vaults below their recorded balances. The one running pool has since been funded (verified on chain). StakePoint states that, of the two ended pools, one is a test pool with no third-party positions and the other is funded; these statements were not independently verified.

06 Statement and limitations

This summary records the retest included in engagement CPK-STAKEPOINT-ENG-001. It covers the program releases identified in Appendix A, deployed at slots 454638982 and 454670815, and reflects evidence through 9 October 2026. It does not cover later changes, deployment configuration, off-chain infrastructure, the frontend, dependencies or third-party components except where expressly stated.

The retest verified each remediated finding by source review and, where the fix is reachable in an isolated runtime, by signed transactions against the deployed executable. The runtime is an in-process Solana runtime with synthetic assets, not a validator or live network. The deployed executables match StakePoint's release record; reproducing them from source is a release-identity step that remains with StakePoint under the engagement letter.

A security assessment identifies vulnerabilities discoverable within its scope, codebase and time frame. No assessment can guarantee that all vulnerabilities have been found, and a resolved or mitigated status is not a warranty, certification or guarantee that the code is free of defects or secure against all attacks. References to an audit describe this security assessment and penetration test; CPK Solutions is not acting as auditor of record.

This summary is prepared for StakePoint under engagement CPK-STAKEPOINT-ENG-001 and should be read with the 7 October 2026 report. StakePoint may share it only in full and unaltered; it must not be excerpted or presented as covering any release other than those identified here. No other person may rely on it, and CPK Solutions accepts no duty or liability to any third party. It is not an endorsement of StakePoint or its tokens, and it is not investment advice.

ISSUED BY

Christopher Kuntz, Principal, CPK Solutions. 9 October 2026.

Appendix A Identities

Item	Value
Program ID	gLHaGJsZ6G7AXZxoDL9EsSWkRbKAWhFHi73gVfNXuzK
ProgramData	46XyGNqwPScDoeayDVWZrkKpvn4eUBdvrB3SY2TRReAm
Upgrade authority	9BMgyCjMsPmSTedyJtc6B1VaFqHugyHQsbbMADMGSHbF (a Squads 3-of-4 multisig, per StakePoint)
Repository	github.com/shaunking1988/stakepoint-audit, branch main
Assessed source	Commit 35ccb5a, lib_current_deployed.rs, SHA-256 19315a4c45759b3d8f9d0cbc3703a939b273cf7afe5c48e2e7be72dc8b2574a7
Release 1 source	Commit 7b74ad1, lib_remediated_2026-10-08.rs, SHA-256 33df2c62aa464342adc85424ba70b7acc73ca5be68c6234d104800003fc44d47
Release 1 executable	Slot 454638982, 1,065,104 bytes, SHA-256 2d820fdb5fa61fb403581e642c1e068dccdcebae8f5cdb461e60e6fcd5740c2e
Release 2 source	Commit e18ec06, lib_remediated_2026-10-08.rs, SHA-256 516afcfb90508e4125302deee102f94eacf867fd7f8989c3d801c4759c54821c
Release 2 executable	Slot 454670815, 1,063,728 bytes, SHA-256 1eb79f89c32135da2c2b53621e0890b527b94988cdb4c819c12847d8691d875e. Current deployment at the evidence cutoff.

Appendix B Retest record

Item	Value
Runtime	Pinned offline runtime image sha256:14310c7505f6..., network disabled, synthetic keys, mints and balances
Final run	run-dbc32a7165824c51a809bfa181f0c3da against the release 2 executable: 38 of 38 suites passed, 264 transactions (242 expected successes, 22 expected rejections), 382 of 382 checks passed
Release 1 run	run-a02a2279d5684b4484d64d80af86a814 against the release 1 executable: 39 of 39 suites passed, 264 transactions, 397 of 397 checks passed
Retained records	Run reports, raw transaction receipts, the reviewed source diff and the on-chain reads are retained by CPK Solutions and available to StakePoint on request.