

FORGE PROTOCOL

FORGE-SEC-2026-11-15

PRODUCTION SECURITY ASSESSMENT

Security Assessment

Active Flare application, hpFLR contracts, services and operating boundaries

PASS FOR ACTIVE FLARE SCOPE

Review participant: Jon-Sn0w
Environment: Codex Daybreak Blue

Flare C-chain · ID 14
15 November 2026 UTC

Active Flare production release

Assessment field	Record
ID	FORGE-SEC-2026-11-15
Date	15 November 2026 UTC
Network	Flare C-chain, chain ID 14, and P-chain staking
Reviewed source	TheForge `main` commit `df0cc542fe99458d0d2236a55343ceefe4fd5639`
Target	Deployed Forge Pages and quote paths, hpFLR contracts, staking and reward services, custody controls, and production configuration
Result	**PASS for the reviewed production source and operational standby; zero confirmed findings remain open**
Reviewer participant	Jon-Sn0w, project owner, using Codex Daybreak Blue

Opinion

The reviewed mainnet production source and effective installed paths have no open confirmed Critical, High, Medium or Low finding. The audit traced the complete active Flare execution graph through contract accounting, native staking authorization and recovery, reward entitlement calculation and claims, swap routing, Pages and browser controls, gas funding, monitoring, and the administrative switch. The globally paused stack is suitable as a reviewed operational standby for an authorized activation decision. This opinion applies to the identified code and observed configuration, not to later deployments or a transaction that has not occurred.

The operational switch remained globally paused at the final read-only check. The reviewed successor MIRROR distributor had four opened epochs, the successor validator-lot distributor had none, and no new holder payout was represented as a completed mainnet event. An opened epoch without funded rewards is not a holder allocation. No stake, payout, key operation, deployment or source edit was performed by the remote reviewer.

Reviewed identity and coverage

The full inventory reconciled **3,316 source files**: 302 executable, dependency and wiring paths included in the active Flare graph and 3,014 individually justified exclusions. It also reconciled 35 required service

instances and 19 active timers, for 356 review rows. Included paths covered the running contracts and pinned dependencies, browser code, Pages and backend code, staking and custody, quotes, rewards and delivery, gas and monitoring, and release wiring. The inventory was limited to paths reached by active chain-14 production execution.

The audited effective Vault proxy is `0x9887BB9BF2871CF637A88b6837429B991CAc803f`; it reads successor operations controller `0x7Ce98385F287B2928f76A39a1C145c3Fd5Ae3a3E` and threshold custody `0xFdD5F0B19704441E807cf512889FEACB8331dEEB`. The OperationalSwitch is `0x10A383318622E730A68D3066266097507f0bE90D`. The MIRROR distributor is `0xa14798A9e69431B2f187341D0C49EF9797b079AF`; the validator-lot distributor is `0x4B41940C0EE26D911F4Ba8BC2d6892C54dA61925`. The installed quote runner hash was `c0ac3171e42ffde4f064bf341f3b590dd829b00864272004162842c682a7ee7d`; its effective catalog behavior was independently compared with the reviewed source change. The active application assets matched the pinned release manifest.

Procedures and results

Area	Review and result
Principal and FIFO	Traced 1:1 mint/burn authority, physical reserve, recognized reward liabilities, funded queue claims, mature lot return, FIFO reservation and restake priority. Cross-module source and adversarial tests passed.
Native staking and custody	Traced typed 2-of-3 approvals, successor signer source, exact node/amount/term/owner binding, three-share custody policy, submission journals, recovery and signer replacement. The installed production roles and current checkpoint were observed; the switch remained paused.
MIRROR, validator rewards and claims	Traced official reward receipt to funded distributor, historical holder snapshots, allocation artifact, root quorum, proof publication, cumulative ledger credit and owner-authorized delivery. The effective materializer and focused 21/21 cases passed; no unearned epoch was inferred from a schedule.
Swap, catalog and wallet	Traced private-node pool indexing through authenticated connector, gateway, Pages catalog and quote, browser preflight, wallet signing and factory-authenticated executor. Completed catalog snapshots are rechecked against the canonical block hash before publication. Catalog and connected tests passed; public catalog and quote blocks matched the private Flare node.
Monitoring and gas	Checked the active service and timer inventory, pinned remote watcher health, current checkpoints, stopped/stalled service detection, and gas funding boundaries. Focused health and gas tests passed; observed monitoring status had no finding.
Governance and release identity	Checked proxy and implementation hashes, roles, successor bindings, the paused switch, interim administration and timelock, installed runtime paths, and public asset hashes against current records. No current operational misconfiguration was identified.

The public catalog check returned chain 14, complete discovery of 2,809 pools and 1,435 tokens across seven venues, with its block hash independently matching the owner's private node. The read-only quote path returned a canonical block and a funded-account preflight was not attempted. The focused catalog verification concluded with **no new finding**. The full review and focused verification together support this

current source and installed standby opinion; the unchanged paths were not pointlessly rerun through the entire suite.

Authority, boundaries and verdict

The production timelock has a 60-second minimum delay. The direct interim administrator remains active and may act under its on-chain authority until forfeiture; this is the intended interim policy and is an explicit trust dependency. Two independently held custody shares are needed for native authorization. Off-chain reward calculations and posted roots require reproducible historical data and independent checking; on-chain funded caps and proofs do not by themselves prove that an operator chose the correct historical balances. Validator availability, RPC integrity, signer hosts, and liquid principal for FIFO exits remain operational dependencies.

The verdict concerns the identified installed production source and configuration. A later contract deployment, policy registration, operator configuration or transaction has its own resulting state and must be verified when executed. This assessment does not claim a first live stake, funded reward period or payout, and does not claim that unknown vulnerabilities are impossible.

Final verdict: PASS for the identified active Flare production source and paused operational standby. No confirmed audit finding remains open.