



FORGE PROTOCOL

FORGE-SEC-2026-10-26

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
26 October 2026 UTC

Active Flare production release

Assessment field	Record
ID	FORGE-SEC-2026-10-26
Date	26 October 2026 UTC
Network	Flare C-chain, chain ID 14
Target	Live Forge application, hpFLR contracts, reward workers and operating controls
Result	PASS - no confirmed Critical, High or Medium finding remains open in the defined active scope
Reviewer participant	Jon-Sn0w, project owner, using Codex Daybreak Blue

Assessment conclusion

The active Forge and hpFLR release passed the defined security review. The review traced principal, reward and wallet value flows through their contract, service and browser boundaries. It exercised adverse state transitions, cross-module accounting, authorization and recovery paths, then checked the reviewed release against finalized Flare bindings and installed services. The conclusion applies to the live release identified below.

The Vault remains a one-to-one hpFLR principal system. Native staking and validator rewards are accounted separately from principal. Available Vault liquidity serves FIFO exits before new staking. The first 50,250 FLR delegation has returned to the Vault, and a legacy validator reward canary has a finalized holder-payment receipt.

Live release identity

Component	Finalized production identity
Vault proxy	0xA71ee4AbcfF4Aa3Ac81BcAE15EE74313f564143
Cumulative MIRROR source	0x92726E4C6b9B7e7c5Bb13d9CD1799BAce718CEF
Cumulative validator source	0xe8216F45a3FE9CE115626F373e9E30A3e1183DaC

Component	Finalized production identity
Cumulative holder ledger	0xA0770d1405cBbfB233B164f0cDbf04916583e988
Governance cutover	Finalized execution 0xbd51e91262411d917584aa9695ba5c42548fe00565e91f996abcdbfb43a31e77
Finalized binding checkpoint	Block 72,981,358; Vault, sources, ledger approvals and roles matched the reviewed release
Production workers	Three independently keyed watchers, proposer, calculator, relay, claimant, two proof publishers and materializer active on their designated hosts

The old cumulative ledger had zero lifetime credits and zero unpaid balance at the cutover checkpoint. Its former sources and posting roles were retired. The successor sources are bound to the new ledger; their poster and claimant roles are active. The installed service health monitor reported no findings.

Audit scope and controls

Area	Reviewed controls and result
Principal and redemption	One-to-one mint and burn, Vault solvency, FIFO reservation and settlement, callback order, reward separation, and claim availability under pause conditions passed contract and integration checks.
Native staking	Typed two-of-three approval, signer-epoch invalidation, exact destination and term binding, P-chain return reconciliation, recovery-only policy, and custody/service journals passed adverse-path review.
MIRROR and validator rewards	Canonical Flare dependency binding, period closure, secure-round snapshot selection, three-block holder balances, reward recognition, funded roots, proof verification, zero-reward lot handling and rollover ordering passed source and integration checks.
Holder claims	Contract-holder recipient authority, counterfactual wallet recovery, exact-value materialization, one cumulative claim per wallet, restake accounting, reentrancy and claim conservation passed contract and browser checks.
Governance and operations	Runtime hashes, role retirement, atomic guarded cutover, finalized receipts, transaction-journal continuity, separate signer hosts, gas funding and service health passed fork and live binding checks.
Forge application	Quote and wallet-context binding, transfer-fee route selection, transaction construction, Pages Functions, proof publication, browser action gating and built-asset identity passed application and publication checks.

The review used source inspection, targeted adversarial tests, Foundry and application suites, a production-code reward flow with twelve varying holders, a disposable Flare fork of the exact governance batch, and finalized mainnet readbacks. The Solidity release suite recorded 623 passes, zero failures and three documented skips. The Forge contract suite recorded 136 passes; the affected wallet-claim browser and Pages release tests passed. The operational Vault build remained below the EVM runtime-size limit.

Production behavior and trust boundaries

The new cumulative contracts and workers are live. No new funded MIRROR or validator period had posted at the assessment checkpoint because no active stake or delegation had produced a new allocation. The first naturally funded cumulative root, ledger credit and holder claim will be recorded when that income exists. A network period boundary alone creates no entitlement. The executable production-code flow verified credit and claim conservation for both streams; it is identified as simulation evidence, not a mainnet holder payment.

The reward root is calculated from historical blocks outside the C-chain and accepted through governed posting roles. On-chain proofs show that a claim matches the posted root and funded amount; they do not independently derive every holder balance from historical blocks. The beta also retains a 60-second administrative timelock, trusted service hosts and RPC providers, and complete-key P-chain custody. External validators, venues and Flare network components remain dependencies. These are disclosed operating authorities, not eliminated risks.

This assessment records a scoped project security review with a named reviewer participant and reproducible evidence. It does not claim independent third-party certification or guarantee the absence of unknown vulnerabilities.