ForgePad · V12 review, triage of every open finding

Robinhood Chain (4663) · V12 run #8519 · triaged 2026-09-29

ForgePad's contracts on Robinhood Chain (chain 4663) were reviewed with V12, Zellic's autonomous AI auditor (run #8519, all 17 source files, Detect + triage), alongside Slither 0.11.5 and Aderyn 0.6.8. This is an automated review, not a manual audit. V12 reported 110 findings and its own triage marked 82 of them invalid. Every one of the remaining 28 was checked by hand against the code; the verdicts are below.

Outcome. 18 confirmed and fixed, with a test for each. The contracts that held no user money when the review came back (the FORGE staking pool, the stock-paired curve and the direct-launch token implementations: 0 staked, 0 launches, 0 tokens) were replaced on mainnet on 2026-09-29 and verified on Sourcify (exact match). 2 are fixed in the source but the live contract is kept, because the ETH curve holds FORGE's own launch; both need unusual conditions and move no user balance. 8 are acknowledged with the reason given.

ID	SEVERITY	FINDING	STATUS	VERDICT
#294379	Critical	**Owner can sweep all staked FORGE principal** ForgeHolderRewards	Fixed · redeployed	Confirmed. sweepUnregistered now refuses FORGE. Nothing was staked when it was replaced.
#294378	Critical	**Abandoned pot sweep leaves later graduation claims unfunded** IgnitionHoldBonus	Fixed in code · live contract kept	Confirmed. The abandoned sweep now zeroes the pot. Needs a launch left open for 365 days; the live ETH curve (which holds FORGE) keeps the old code, the new stock curve has the fix.
#294148	Critical	**Halt strands pot after all tokens are sold** ForgeIgnitionQuoted	Fixed · redeployed	Confirmed. With nothing sold the pot stays for the sweep instead of merging into an unredeemable reserve.
#294249	Critical	**Untracked ETH can be permanently stranded** ForgeIgnition	Fixed in code · live contract kept	Confirmed, low impact: ETH sent to the contract by mistake, and rounding dust refunded at graduation, have no withdrawal path. No user balance is affected. Recovery path planned for the next curve version.
#294085	High	**Quoted fee payouts can block trades** ForgeIgnitionQuoted	Fixed · redeployed	Confirmed. A payout the asset refuses (issuer blocklist, rejecting hook) is now kept as owed and withdrawable; it can no longer revert a trade.
#294358	High	**Reverting quoted-fee recipients can halt curve trading** ForgeIgnitionQuoted	Fixed · redeployed	Same fix as #294085.
#294401	High	**Unchecked uint128 casts corrupt curve and bonus accounting** ForgeIgnitionQuoted, IgnitionHoldBonus	Fixed · redeployed	Confirmed for tokens with more than 2^128 units (open pairs only). All narrowing now uses SafeCast. Not reachable on the ETH curve.
#294146	High	**Graduation vulnerable to fee-on-transfer quote assets** ForgeIgnitionQuoted	Acknowledged	Open pairs only (any token the creator chooses). Verified pairs are Robinhood stock tokens without transfer fees. Open pairs are marked unverified with an explicit risk warning.
#294396	High	**Nominal outbound payouts underpay for lossy quote tokens** ForgeIgnitionQuoted	Acknowledged	Same scope and mitigation as #294146.
#294335	High	**Native deposits forge token claims** ForgeDividendToken	Fixed · redeployed	Confirmed and serious: 1 wei of ETH could make every reflection claim revert, or drain an ERC-20 reward pool. ETH is now refused unless holders are paid in ETH. 0 such tokens existed.
#294336	High	**Threshold changes leave stale shares** ForgeDividendToken	Fixed · redeployed	Confirmed. Claiming syncs shares first; anyone can sync an account.

#294339	High	**Unbounded shares break dividend arithmetic** ForgeDividendToken	Fixed · redeployed	Confirmed for extreme supplies. Supply is now capped at 2^112 units.
#294340	High	**Eligibility deadlock permanently traps rewards** ForgeDividendToken	Fixed · redeployed	Mitigated: the minimum balance is capped against circulating supply (burned tokens excluded).
#294351	High	**Native payout failures can block or forfeit entitlements** several	Fixed · redeployed	Staking: claimTo lets a staker send rewards to another address. Curve sells and creator claims pay the caller's own address by design.
#294356	High	**Reward synchronization strands rounding residuals** ForgeHolderRewards	Fixed · redeployed	Confirmed (dust). The remainder is now carried to the next sync.
#294380	High	**A failing reward asset blocks claims for all assets** ForgeHolderRewards	Fixed · redeployed	Confirmed. claimTo(to, assets) claims asset by asset.
#294357	High	**Synchronous fee payouts can freeze locked-position collection** ForgeLockedLiquidity	Acknowledged	Confirmed for stock-paired pools whose creator is blocklisted by the stock's issuer: that one position's fees wait. Other positions are unaffected. The locker is bound to the manager and cannot be replaced; deferred payouts are planned for its next version.
#294368	High	**Whole-balance refunds let callers sweep manager assets** ForgeV4LiquidityManager	Acknowledged	Confirmed. Only affects assets left in the manager by mistake; it holds nothing between operations.
#294388	High	**Spot-derived buyback floor permits sandwich attacks** ForgeFlywheel	Acknowledged	Design limitation. Configured at 0.25 ETH per call, 1 hour apart; these are settings the owner can change, not hard limits. A round trip pays 0.8–1% twice in fees. The relaunch makes the limits constants and prices the buyback over two points 30 minutes apart.
#294293	Medium	**Blocked assets bypass curated admission** ForgeIgnitionQuoted	Fixed · redeployed	Confirmed. Every launch path now refuses a blocked asset.
#294398	Medium	**Owner can force healthy launches into redemption** ForgeIgnitionQuoted	Fixed · redeployed	Confirmed. halt() now requires the asset to be publicly blocked first.
#294331	Medium	**Pair label bypasses sell-tax ban** ForgeTokenBase	Fixed · redeployed	Confirmed. On Robinhood Chain no second pair can be added and a transfer into the pool is always a sell.
#294332	Medium	**Unbounded limits can freeze holders** ForgeTokenBase	Fixed · redeployed	Confirmed. Limits are capped at 100%.
#294338	Medium	**Payout callback bypasses token controls** ForgeDividendToken	Fixed · redeployed	Confirmed. ETH and ERC-20 payouts no longer run under the swap lock.
#294341	Medium	**Distribution remainders are permanently stranded** DividendPayingUpgradeable	Fixed · redeployed	Confirmed (dust). The remainder stays queued for the next distribution.
#294034	Low	**View quotes can revert on zero-amount inputs** ForgeIgnition, IgnitionCurve	Acknowledged	View functions only; trades are unaffected.
#294361	Low	**Trade quotes can report outcomes that execution rejects** ForgeIgnitionQuoted	Acknowledged	Quotes are estimates; the app applies the caps before sending.

#294362	**Low**	**Wallet cap checks gross rather than net amount** ForgeTokenBase	Acknowledged	Conservative: a cap can bind slightly early on a taxed buy.

Contracts on mainnet after the fixes

ForgeHolderRewards (new)	`0x162c33B5CffE8DbBCDE81d56451D5716f7218DC2`
ForgeIgnitionQuoted (new)	`0xA069C601Ee2488BCEC0231CB54c543ae38b43768`
ForgeToken implementation (new)	`0xD4362172BdC0682186CF82df77866E9850A74719`
ForgeDividendToken implementation (new)	`0xF8784ae43773ed34D3842237F10D3d731Ba11445`
ForgeIgnition	`0x705c4c9Ce2655fFD43a7B9b54a7797e054997dEe`
ForgeRevenue	`0xA498A983efC97FDC247FfB3abA74f6be0fECE9EE`
ForgeV4LiquidityManager	`0xD52B45078Bb2b5C41f046d18EADb95B703Dc478a`
ForgeLockedLiquidity	`0x2465C87304711f732b0Df1C6F27925bc8cb16af9`
ForgeFlywheel	`0x89844AF35cC2507891d606223cCEBd4224DD3433`
ForgeTokenFactory	`0x93C20669391F1B2E3f7e6E27b05deEeB8F1757B8`
FORGE	`0xb9a49A9ca3bb856d71a5f7E46Afb4232C58ba221`

Verified sources: repo.sourcify.dev/4663/<address>. Fix commit: ForgePad 2b02a132. V12's own export of all 110 findings is published next to this report.