



FULL-STACK SECURITY REVIEW

SECURITY REVIEW —

· Track T1 —

/ BoringVault RWA vault suite

PROJECT



TRACK / TIER

T1 · Full

DATE

7 April 2026

CHAINS

Ethereum + additional EVM
chains (LayerZero / Hyperlane
/ OP)

CODE VERSION

locked at kickoff (pending)

CLASSIFICATION

PUBLIC SAMPLE

Disclaimer. This report describes a time-boxed technical security review of the materials identified in the Scope of Review as they existed at the referenced commit/version during the review window. It is a point-in-time assessment: subsequent changes to code, configuration, infrastructure, or dependencies are not covered. No security review can identify all vulnerabilities. This report does not constitute a guarantee, warranty, or insurance of any kind, and it is not an endorsement of the project, its business model, or its tokens. It is not investment, legal, or financial advice. The review does not include formal verification, continuous monitoring, or exhaustive novel economic attack modeling unless expressly stated in scope. ■■■ may publish or share this report in full, unmodified form, including this disclaimer. Partial reproduction that omits findings, statuses, or this disclaimer is not authorized. Vari accepts no liability for decisions made by third parties on the basis of this report.

00 EXECUTIVE SUMMARY

██████ is a Veda / Se7en-Seas “Arctic Architecture” BoringVault fork adapted into a permissioned, KYC-gated, cross-chain RWA vault whose share price grows by an administered lending rate rather than realized asset performance. The inline “audit-X fixed” hardening is genuine and present (Accountant reject-without-commit, Teller dual-side access checks and fail-closed ██████, AtomicSolver drain guards, Manager flash-loan pinning, cross-chain peer enforcement). Residual risk is concentrated in items the project’s own ██████ still marks DEFERRED: no permissionless emergency exit, a cross-chain entry path that bypasses KYC/cap/share-lock, and an exchange rate decoupled from real backing that keeps accruing while paused.

CRITICAL 0	HIGH 2	MEDIUM 2	LOW 4	INFO 0
---------------	-----------	-------------	----------	-----------

Highest-priority items: **PROTO-T1-01** No permissionless emergency exit — every withdrawal path is keeper/solver-gated; **PROTO-T1-02** Cross-chain entry bypasses KYC (checkAccess), deposit cap and share-lock.

01 SCOPE OF REVIEW

BoringVault, TellerWithMultiAssetSupport (+ OP / LayerZero / Hyperlane cross-chain tellers), ManagerWithMerkleVerification, AccountantWithRateProviders, AtomicQueue / AtomicSolverV5, DEX micro-managers, decoders & sanitizers, rate providers/oracles. ~162 files / ~12.3K SLOC. Funds-holding, multi-chain.

TRACK :: T1 · TIER :: Full · CHAINS :: Ethereum + additional EVM chains (LayerZero / Hyperlane / OP) · CODE :: locked at kickoff (pending)

Out of scope: third-party dependencies (base libraries, external protocols, bridge/oracle endpoints), off-chain keeper/relayer infrastructure, and key management, assumed correct unless expressly listed. Test, mock and deploy-script files were read for context but are not the subject of the findings.

02 METHODOLOGY

AI-assisted broad analysis over the full source followed by targeted human review of business logic, value-moving paths, roles/permissions and higher-risk areas; cross-layer reconciliation; and live-state verification of the deployed settings (see §05). The review is manual + AI-assisted + static; it does not include formal verification or runtime fuzzing unless stated. Severity reflects exploitability + impact, never effort: **Critical** (direct path to loss of funds / full compromise) · **High** (exploitable, realistic conditions, material impact) · **Medium** (limited impact or unusual preconditions) · **Low** (defense-in-depth / best practice) · **Info** (observation).

03 FINDINGS

ID	SEVERITY	LAYER	FINDING
PROTO-T1-01	HIGH	contracts	No permissionless emergency exit — every withdrawal path is keeper/solver-gated
PROTO-T1-02	HIGH	cross-chain	Cross-chain entry bypasses KYC (checkAccess), deposit cap and share-lock

PROTO-T1-03	MEDIUM	contracts	Administered exchange rate decoupled from backing; accrual not frozen on pause
PROTO-T1-04	MEDIUM	contracts	Flash-loan continuation verified against manageRoot[manager], not the initiating strategist
PROTO-T1-05	LOW	contracts	AtomicQueue removed per-user limit-price floor; users redeem at live admin NAV
PROTO-T1-06	LOW	contracts	Dust request rounding to zero want reverts the whole solve batch
PROTO-T1-07	LOW	config	EthPerTokenRateProvider has no L2 sequencer-uptime guard
PROTO-T1-08	LOW	contracts	KYC not enforced on share custody/transfers; wrappers collapse per-user checks

HIGH

PROTO-T1-01

No permissionless emergency exit — every withdrawal path is keeper/solver-gated

LOCATION

```
TellerWithMultiAssetSupport.bulkWithdraw (requiresAuth SOLVER_ROLE); AtomicQueue.solve (requiresAuth SOLVER_ROLE)
```

DESCRIPTION

There is no user-callable redeem. Users can enter, but the only exits require a trusted keeper. If keepers halt, the accountant auto-pauses, or governance pauses the Teller/Manager, depositor funds are inaccessible with no on-chain fallback. The project's █████ flags this (R-1) as the single most important DEFERRED critical and states it "blocks a production mainnet redeploy."

IMPACT

Under keeper outage, pause, or governance inaction, user funds are locked indefinitely with no permissionless recovery. Liveness/censorship risk on principal.

RECOMMENDATION

Add a permissionless, rate-based emergency redeem gated only by solvency, or a time-locked escape hatch that activates after the system has been paused beyond a threshold.

Status: OPEN · Confidence: high — verified in code; corroborated by █████ R-1

HIGH

PROTO-T1-02

Cross-chain entry bypasses KYC (checkAccess), deposit cap and share-lock

LOCATION

```
CrossChainTellerBase.depositAndBridge; MultiChainLayerZero receive / Hyperlane handle / OP  
receiveBridgeMessage (vault.enter direct)
```

DESCRIPTION

deposit/depositWithPermit/bulkDeposit/bulkWithdraw all carry checkAccess, but depositAndBridge() and the destination receive handlers do not: they mint shares with no access check on sender or receiver, no deposit-cap enforcement, and no shareUnlockTime. A non-KYC/sanctioned address can mint shares via the bridge path and be solved out. This is the still-DEFERRED T-1 the team labels critical.

IMPACT

The KYC/whitelist, deposit cap and anti-MEV share-lock — the core compliance and risk controls of a regulated vault — are bypassable through the cross-chain path.

RECOMMENDATION

Add checkAccess(msg.sender) to depositAndBridge; on receive, mint into a claim quarantine that enforces checkAccess(receiver) + cap + per-lot unlock at claim time rather than minting directly.

Status: OPEN · Confidence: high — verified: checkAccess absent in CrossChainTellerBase and all receive handlers

MEDIUM

PROTO-T1-03

Administered exchange rate decoupled from backing; accrual not frozen on pause

LOCATION

```
AccountantWithRateProviders.calculateExchangeRateWithInterest / _checkpointInterestAndFees  
/ setMaxLendingRate
```

DESCRIPTION

The rate grows deterministically by $\text{lendingRate} \times dt$ independent of realized repayments and is committed on every deposit/withdraw with no bound check and no auto-pause (those rails only guard manual updates). Pause blocks state writes but the time-based accrual is not frozen, so a paused window compounds on unpause. Management fees leave the vault without reducing the rate. setMaxLendingRate has no upper cap.

IMPACT

The rate can diverge from actual assets. On default or fee drain, early withdrawers redeem inflated NAV at later depositors' expense (first-redeemer / bank-run dynamic).

RECOMMENDATION

Freeze last-accrual time on pause; drive accrual from realized repayments (or add a write-down that can lower the rate on default); cap setMaxLendingRate; reduce rate (or track NAV separately) when fees exit.

Status: OPEN · Confidence: high — verified; matches A-5

MEDIUM

PROTO-T1-04

Flash-loan continuation verified against manageRoot[manager], not the initiating strategist

LOCATION

```
ManagerWithMerkleVerification.receiveFlashLoan → self-call  
manageVaultWithMerkleVerification; _verifyCallData uses manageRoot[msg.sender]
```

DESCRIPTION

The self-re-entrant continuation runs with `msg.sender ==` the manager, so in-loan calls are gated by `manageRoot[manager]` rather than the initiating strategist's own root. Per-strategist scoping is lost inside flash-loan callbacks.

IMPACT

Whoever configures `manageRoot[manager]` effectively defines what any flash-loan continuation may do, potentially broader than the initiating strategist's permissions.

RECOMMENDATION

Pass the initiating strategist through the flash-loan intent and verify the continuation against that strategist's root, or keep `manageRoot[manager]` deliberately minimal and verify it on-chain.

Status: OPEN · Confidence: med — code path confirmed; exploitability depends on `manageRoot[manager]` config

LOW

PROTO-T1-05

AtomicQueue removed per-user limit-price floor; users redeem at live admin NAV

LOCATION

```
AtomicQueue.updateAtomicRequest / _calculateWantAmount
```

DESCRIPTION

The upstream `AtomicRequest` carried a user-set price floor; this fork removed it (requests store `deadline + offerAmount` only, want computed from the live rate at solve). The solver cannot underpay within a solve, but a user has no protection against an adverse rate move between submission and solve, bounded only by the deadline.

IMPACT

Users bear all rate movement between request and solve with no on-chain minimum; solve timing is chosen by the (trusted) solver.

RECOMMENDATION

Reintroduce an optional user-specified minimum want amount and enforce it at `finalize-solve` (skip rather than revert when unmet).

Status: OPEN · Confidence: high — design change verified vs upstream

LOW

PROTO-T1-06

Dust request rounding to zero want reverts the whole solve batch

LOCATION

```
AtomicQueue._prepareSolve (revert on zero output)
```

DESCRIPTION

Submission-time checks validate `deadline/balance/allowance` but not `want>0`; at solve time a single request whose offer rounds to zero want reverts the entire batch, and rate drift reopens this even with a submission check. Honest keepers must filter off-chain.

IMPACT

Griefing/DoS on keeper solve batches; degraded exit liveness (compounds PROTO-T1-01).

RECOMMENDATION

Implement the deferred skip-and-emit so zero-output requests are skipped instead of reverting the batch.

Status: OPEN · Confidence: high — verified; matches █████ Q-2/I-2

LOW PROTO-T1-07 **EthPerTokenRateProvider has no L2 sequencer-uptime guard**

LOCATION

```
oracles/EthPerTokenRateProvider._validityCheck (empty virtual)
```

DESCRIPTION

getRate enforces Chainlink/Redstone staleness and rejects non-positive answers, but the _validityCheck hook meant for sequencer liveness is an empty virtual. On an L2 without an override, a down/recovering sequencer can serve stale-but-in-window prices.

IMPACT

Stale pricing on L2 deployments during sequencer downtime; mispriced entries/exits.

RECOMMENDATION

Deploy an override that checks the L2 sequencer-uptime feed and grace period on any L2; verify per deployment.

Status: OPEN · Confidence: med — deploy-dependent; code shows no guard

LOW PROTO-T1-08 **KYC not enforced on share custody/transfers; wrappers collapse per-user checks**

LOCATION

```
BoringVault._callBeforeTransfer / Teller.beforeTransfer(from);  
helper/WarpRouteWrapper.depositAndBridge
```

DESCRIPTION

beforeTransfer only checks the sender's share-lock, not recipient KYC, so KYC gates deposit/withdraw flows but not who may hold shares. WarpRouteWrapper deposits as itself, so only the wrapper's contract-whitelist status is checked (not the end user), minting fresh shares for an unchecked caller.

IMPACT

Compliance cannot rely on the KYC mode to restrict holders; a whitelisted wrapper/contract becomes an unchecked minting funnel (related to PROTO-T1-02).

RECOMMENDATION

If holder-level compliance is required, enforce checkAccess on transfer recipients and pass the true end-user through wrappers (or drop contract-whitelist for minting paths).

Status: OPEN · Confidence: high — verified in code

04 WHAT'S SOLID

- Accountant reject-without-commit + checkpoint-below-bound on updateExchangeRate: a bad rate pauses without persisting; upper/lower change caps (11000/9000 bps) enforced; rate-provider replacement deviation-checked to 5%.
- Teller bulkWithdraw checks BOTH msg.sender (solver) and _to; [REDACTED] fails closed when the [REDACTED] is unset; bulkDeposit/bulkWithdraw honor isPaused; dust deposits that round to zero shares revert.
- AtomicQueue.solve pins solver == msg.sender; AtomicSolverV5 layers approvedQueues + in-solve context + expected-queue against the known drain class, with fee-on-transfer reconciliation.
- Manager pins flash-loan recipient to self and validates an intent hash; manage() enforces a constant-total-supply invariant across the batch; LayerZero/Hyperlane/OP receives enforce peer/mailbox/messenger authenticity.
- isReceivePaused decoupled from isPaused so a destination-side pause cannot black-hole in-flight bridged shares (fixes the parallel of a known [REDACTED]-class issue).

05 LIVE ON-CHAIN VERIFICATION

Pending deployed addresses. Governance/config findings must reflect the deployed state, not the source. The items below are queued to be read live (via Etherscan V2 proxy `eth_call`) once [REDACTED] provides the deployed addresses + chains per system; each will be reported PASS / ACTION / VERIFY / INFO. Until then they are marked VERIFY.

- RolesAuthority wiring: which selectors are public (esp. deposit / depositAndBridge / bridge) vs role-gated; confirm depositAndBridge is not publicly callable given it lacks checkAccess.
- accessControlMode per Teller; [REDACTED] + policyId set before [REDACTED] is enabled; contents of manual/contract whitelists (any wrapper/solver present?).
- Accountant live state: paused, exchangeRate vs actual backing, lendingRate, maxLendingRate, managementFee, allowed change bounds, minimum update delay, payout address.
- rateProviderData per asset (pegged flags, provider addresses); on L2s, whether the rate provider overrides the sequencer-uptime check.
- Manager: manageRoot per strategist AND manageRoot[manager]; Manager/Teller/Accountant pause states; holders of SOLVER / UPDATE_EXCHANGE_RATE / OWNER / MULTISIG roles.
- Cross-chain config consistency: LayerZero peers vs targetTeller vs allowMessagesFrom/To; Hyperlane mailbox/ISM; OP messenger/peer; depositCap set (>0) on every chain.

06 ACTION POINTS

PRIORITY	ID	ACTION	STATUS
P0	PR0T0-T1-01	No permissionless emergency exit — every withdrawal path is keeper/solver-gated	◦ OPEN
P0	PR0T0-T1-02	Cross-chain entry bypasses KYC (checkAccess), deposit cap and share-lock	◦ OPEN
P1	PR0T0-T1-03	Administered exchange rate decoupled from backing; accrual not frozen on pause	◦ OPEN
P1	PR0T0-T1-04	Flash-loan continuation verified against manageRoot[manager], not the initiating strategist	◦ OPEN
P2	PR0T0-T1-05	AtomicQueue removed per-user limit-price floor; users redeem at live admin NAV	◦ OPEN
P2	PR0T0-T1-06	Dust request rounding to zero want reverts the whole solve batch	◦ OPEN
P2	PR0T0-T1-07	EthPerTokenRateProvider has no L2 sequencer-uptime guard	◦ OPEN
P2	PR0T0-T1-08	KYC not enforced on share custody/transfers; wrappers collapse per-user checks	◦ OPEN

P0 = before deploy / now · P1 = soon · P2 = hardening. Status column is filled at the re-review round (report goes to v1.1: ◦ OPEN · ✓ FIXED · ~ ACKNOWLEDGED · ✗ NOT FIXED).

07 RESIDUAL RISK

After the recommended fixes, residual risk concentrates in the privileged roles (owner/manager/strategist/governor keys) and in operational posture — key custody, multisig thresholds, timelocks, and monitoring — which code alone cannot guarantee. Because this system holds user funds, a companion Economic Modeling Addendum accompanies this report and models the solvency and adverse-market mechanics summarized above. This is a point-in-time review; re-verify after any change to code, configuration, or deployed settings.

VARI — EVERY LAYER. ONE REVIEW.

██████ · T1 ██████ · 7 April 2026

CLASSIFICATION :: PUBLIC SAMPLE — CLIENT IDENTITY REDACTED · CONTACT :: TELEGRAM @va_rinder ·
VARIEREVIEW.COM