

Lotus Security Audit Summary

Prepared by Cyfrin

Version 2.0

Head of Security Research

Dacian (Proprietary AI)

Lead Auditors

Stalin

Kiki

BenRai

JuliusRaynaldi (Formal Verification)

November 12, 2026

Contents

1 About Cyfrin **2**

2 About This Document **2**

3 Disclaimer **2**

4 Copyright and License **2**

5 Audits at a Glance **3**

6 Protocol Summary **4**

7 Lotus First Audit **5**
7.1 Overview . . . 5
7.2 Audit Details . . . 5
7.3 Audit Scope . . . 5

8 Lotus Second Audit **8**
8.1 Overview . . . 8
8.2 Audit Details . . . 8
8.3 Audit Scope . . . 8

9 Post-Audit Solace Scan and Remediation Review **9**
9.1 Overview . . . 9
9.2 Review Details . . . 9
9.3 Scan Scope . . . 9

10 Attestation **12**

1 About Cyfrin

Cyfrin is a Web3 security company dedicated to bringing industry-leading protection and education to our partners and their projects. Our goal is to create a safe, reliable, and transparent environment for everyone in Web3 and DeFi. Learn more about us at cyfrin.io.

2 About This Document

This document is a public summary of the two security audits Cyfrin performed for Lotus Labs on the Lotus protocol and a subsequent Solace proprietary-AI scan with targeted remediation review. It records the repositories and commits reviewed, the timelines, auditors, in-scope files, and the finding counts and statuses by severity. The Solace scan is presented separately from the two audits, with resolved and acknowledged findings distinguished. It closes with Cyfrin's attestation of the documented scopes, reviewed revisions and reported statuses. It supersedes the two standalone audit reports as the shareable record of these engagements.

Technical details of individual findings are omitted from this public summary to limit disclosure of security-sensitive information. The complete report, with every finding of both audits and of the Solace scan, was delivered privately to Lotus Labs, who retain it as the full record of these engagements. Recipients of the full report can use the SHA-256 hash in this summary's attestation to confirm that their copy matches the referenced report.

3 Disclaimer

The Cyfrin team makes every effort to find as many vulnerabilities in the code as possible in the given time but holds no responsibility for the findings in this document. A security audit by the team does not endorse the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the in-scope code being audited. Unless the scope explicitly notes otherwise, the review is limited to the application layer and does not extend to the correctness of API/SDK/execution environment implementations, compilers, standard and third-party libraries, underlying operating systems and hardware.

An audit is a point-in-time review of a specific revision of the code. It is not a guarantee that the code is free of vulnerabilities, and it says nothing about code changed after the reviewed revision.

4 Copyright and License

© 2026 Cyfrin Inc. All rights reserved. Material from Lotus Labs or third parties remains the property of its owners.

This summary may be shared only in complete and unmodified form, so that any copy can be checked against the hash in its attestation. Short quotations with attribution to Cyfrin are permitted, provided they do not misrepresent this summary’s scope or results. Except as permitted by applicable law, no part of this summary may otherwise be copied, modified, adapted, sold or sublicensed, or used to create derivative works, without Cyfrin’s prior written permission.

Cyfrin and the Cyfrin logo are trademarks of Cyfrin Inc. and may not be used to suggest that Cyfrin has reviewed or endorses anything outside this summary’s scope, or to misrepresent its results.

5 Audits at a Glance

Cyfrin performed two audits of the lotus repository for Lotus Labs.

Audits

#	Audit	Audit Timeline	Audit Commit	Final Mitigation Commit
1	Lotus First Audit	June 29th - July 31st, 2026	`5a53cc9`	`e76cde5`
2	Lotus Second Audit	Sep 7th - Sep 16th, 2026	`2226102`	`b15126f`

The final mitigation revision for the two audits is commit `b15126f77a70d1f529e49afa61c2e4abfcc9995d` of the lotus repository.

A subsequent Solace proprietary-AI scan and targeted remediation review are recorded separately in Section 9. Its core-code and deployment-script remediations were reviewed together at commit `4ad5fe3`. Scan findings are not included in the audit totals above.

Issues Found (All Audits)

Severity	Found	Resolved	Acknowledged
Critical Risk	0	0	0
High Risk	6	6	0
Medium Risk	14	14	0
Low Risk	26	23	3
Informational	29	20	9
Gas Optimizations	6	6	0
Total	81	69	12

How to read the statuses

Resolved means Cyfrin verified the remediation documented in the full report with a Cyfrin verification note. Acknowledged means Lotus Labs chose to retain the reported behavior or accept the residual risk; this does not constitute resolution or endorsement by Cyfrin. Finding-specific explanations and verification notes are recorded in the full report.

Risk Classification

	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

6 Protocol Summary

Lotus is a multi-tranche lending protocol. Rather than isolated pools, each Lotus market contains several tranches ordered from senior to junior, each with its own collateral token, oracle and loan-to-value limit, so lenders choose how much risk they take by choosing a tranche. Each market is configured with a risk engine, which sets borrow rates and allocates interest and losses across tranches, and a liquidation module.

Liquidity reaches Lotus markets through Morpho Vault V2 parent vaults, which allocate assets through adapters into Lotus markets, other ERC-4626 vaults and off-chain productive venues. Bundler adapters let users batch Lotus and vault interactions into a single transaction.

7 Lotus First Audit

7.1 Overview

The original audit was a full review of the Lotus codebase at the audit commit, combining manual review with formal verification. Lotus Labs remediated the findings and Cyfrin reviewed the remediation up to the final mitigation commit. Several remediations made substantial changes to the reviewed code, so Cyfrin recommended a follow-up audit before deployment.

7.2 Audit Details

Summary

Repository	lotus
Audit Commit	5a53cc9c2499e88d158ba2b4b843e20d3007ca5e
Final Mitigation Commit	e76cde55198136b6b8088c9bca3f8d7cd14cb301
Audit Timeline	June 29th - July 31st, 2026
Methods	Manual Review, Proprietary AI, Formal Verification
Lead Auditors	Stalin, Kiki, BenRai, JuliusRaynaldi (Formal Verification)

Issues Found

Severity	Found	Resolved	Acknowledged
Critical Risk	0	0	0
High Risk	4	4	0
Medium Risk	13	13	0
Low Risk	19	17	2
Informational	18	17	1
Gas Optimizations	6	6	0
Total	60	57	3

7.3 Audit Scope

The audit scope was limited to:

```
src/Lotus.sol
src/bundler3/AdapterBase.sol
src/bundler3/ERC4626LotusBundlerAdapter.sol
src/bundler3/LotusBundlerAdapter.sol
src/bundler3/interfaces/IAdapterBase.sol
src/bundler3/interfaces/IERC4626LotusBundlerAdapter.sol
src/bundler3/interfaces/ILotusBundlerAdapter.sol
src/factories/ModuleFactory.sol
src/factories/interfaces/IModuleFactory.sol
src/governance/LotusGovernor.sol
src/governance/OperatorTimelock.sol
src/governance/interfaces/ILotusGovernor.sol
src/governance/interfaces/IOperatorTimelock.sol
```

src/hooks/FlowCapHook.sol
src/hooks/interfaces/IFlowCapHook.sol
src/hooks/interfaces/ILotusHooks.sol
src/hooks/libraries/BaseLotusHook.sol
src/hooks/libraries/Hooks.sol
src/interfaces/IBundler3.sol
src/interfaces/IERC20.sol
src/interfaces/IERC20Metadata.sol
src/interfaces/ILiquidationModule.sol
src/interfaces/ILotus.sol
src/interfaces/ILotusCallbacks.sol
src/interfaces/IOracle.sol
src/interfaces/IRiskEngine.sol
src/lens/LotusLens.sol
src/lens/interfaces/ILotusLens.sol
src/libraries/BaseUpgradeableModule.sol
src/libraries/ConstantsLib.sol
src/libraries/InterestMathLib.sol
src/libraries/LotusBalancesLib.sol
src/libraries/LotusErrorsLib.sol
src/libraries/LotusEventsLib.sol
src/libraries/LotusPauseLib.sol
src/libraries/MarketParamsLib.sol
src/libraries/PendingLib.sol
src/libraries/SharesMathLib.sol
src/libraries/UtilsLib.sol
src/liquidations/HealthDiscountLiquidationModule.sol
src/liquidations/OracleIncentiveLiquidationModule.sol
src/liquidations/factories/HealthDiscountLiquidationModuleFactory.sol
src/liquidations/factories/OracleIncentiveLiquidationModuleFactory.sol
src/liquidations/interfaces/IHealthDiscountLiquidationModule.sol
src/liquidations/interfaces/IHealthDiscountLiquidationModuleFactory.sol
src/liquidations/interfaces/IOracleIncentiveLiquidationModule.sol
src/liquidations/interfaces/IOracleIncentiveLiquidationModuleFactory.sol
src/liquidations/libraries/BaseLiquidationModule.sol
src/liquidations/libraries/LiquidationErrorsLib.sol
src/oracles/interfaces/AggregatorV3Interface.sol
src/oracles/interfaces/IBoundedStalenessFeed.sol
src/oracles/staleness/BoundedStalenessFeed.sol
src/pre-liquidation/PreLiquidation.sol
src/pre-liquidation/PreLiquidationFactory.sol
src/pre-liquidation/interfaces/IPreLiquidation.sol
src/pre-liquidation/interfaces/IPreLiquidationCallback.sol
src/pre-liquidation/interfaces/IPreLiquidationFactory.sol
src/pre-liquidation/libraries/PreLiquidationErrorsLib.sol
src/risk-engines/AdaptiveLinearKinkRiskEngine.sol
src/risk-engines/FixedRateRiskEngine.sol
src/risk-engines/ManagedLinearKinkRiskEngine.sol
src/risk-engines/MonotonicAdaptiveLinearKinkRiskEngine.sol
src/risk-engines/MonotonicManagedLinearKinkRiskEngine.sol
src/risk-engines/factories/AdaptiveLinearKinkRiskEngineFactory.sol
src/risk-engines/factories/FixedRateRiskEngineFactory.sol
src/risk-engines/factories/ManagedLinearKinkRiskEngineFactory.sol
src/risk-engines/factories/MonotonicAdaptiveLinearKinkRiskEngineFactory.sol
src/risk-engines/factories/MonotonicManagedLinearKinkRiskEngineFactory.sol
src/risk-engines/interfaces/IAdaptiveLinearKinkRiskEngine.sol
src/risk-engines/interfaces/IAdaptiveLinearKinkRiskEngineFactory.sol
src/risk-engines/interfaces/IBaseLinearKinkRiskEngine.sol
src/risk-engines/interfaces/IFixedRateRiskEngine.sol
src/risk-engines/interfaces/IFixedRateRiskEngineFactory.sol
src/risk-engines/interfaces/IManagedLinearKinkRiskEngine.sol
src/risk-engines/interfaces/IManagedLinearKinkRiskEngineFactory.sol

```
src/risk-engines/interfaces/IMonotonicAdaptiveLinearKinkRiskEngineFactory.sol
src/risk-engines/interfaces/IMonotonicManagedLinearKinkRiskEngineFactory.sol
src/risk-engines/libraries/BaseLinearKinkRiskEngine.sol
src/risk-engines/libraries/BaseRiskEngine.sol
src/risk-engines/libraries/MonotonicUtilLib.sol
src/risk-engines/libraries/RiskEngineErrorsLib.sol
src/risk-engines/libraries/RiskEngineEventsLib.sol
src/vault-v2/LotusAdapterRegistry.sol
src/vault-v2/adapters/CoinbasePrimeAdapter.sol
src/vault-v2/adapters/LotusV2Adapter.sol
src/vault-v2/adapters/VaultV2Adapter.sol
src/vault-v2/adapters/WGTXXAdapter.sol
src/vault-v2/factories/LotusVaultFactory.sol
src/vault-v2/gates/BinaryVaultGate.sol
src/vault-v2/interfaces/IAdapter.sol
src/vault-v2/interfaces/IAdapterRegistry.sol
src/vault-v2/interfaces/IBinaryVaultGate.sol
src/vault-v2/interfaces/ICoinbasePrimeAdapter.sol
src/vault-v2/interfaces/IERC20Skim.sol
src/vault-v2/interfaces/ILotusAdapterRegistry.sol
src/vault-v2/interfaces/ILotusV2Adapter.sol
src/vault-v2/interfaces/ILotusVaultFactory.sol
src/vault-v2/interfaces/ISettlementWindowGate.sol
src/vault-v2/interfaces/ISkimmable.sol
src/vault-v2/interfaces/IVaultV2.sol
src/vault-v2/interfaces/IVaultV2Adapter.sol
src/vault-v2/interfaces/IVaultV2Factory.sol
src/vault-v2/interfaces/IWGTXXAdapter.sol
src/vault-v2/libraries/BaseLotusV2Adapter.sol
src/vault-v2/libraries/Skimmable.sol
```

8 Lotus Second Audit

8.1 Overview

The follow-up audit was carried out in response to the original audit's recommendation and focused on the components that changed the most from the original audit. Cyfrin then reviewed Lotus Labs' remediation of the follow-up findings up to the final mitigation commit, including the changes those fixes required elsewhere in the codebase.

8.2 Audit Details

Summary

Repository	lotus
Audit Commit	22261025568c24869f74855cea56e820359b0b03
Final Mitigation Commit	b15126f77a70d1f529e49afa61c2e4abfcc9995d
Audit Timeline	Sep 7th - Sep 16th, 2026
Methods	Manual Review, Proprietary AI
Lead Auditors	Stalin, BenRai

Issues Found

Severity	Found	Resolved	Acknowledged
Critical Risk	0	0	0
High Risk	2	2	0
Medium Risk	1	1	0
Low Risk	7	6	1
Informational	11	3	8
Gas Optimizations	0	0	0
Total	21	12	9

8.3 Audit Scope

The audit scope was limited to:

```
// Planned V1 Risk Engine
src/risk-engines/MonotonicManagedLinearKinkRiskEngine.sol
src/risk-engines/ManagedLinearKinkRiskEngine.sol
src/risk-engines/libraries/BaseLinearKinkRiskEngine.sol
src/risk-engines/libraries/BaseRiskEngine.sol

// Selected Vault Adapters
src/vault-v2/adapters/WGTXXAdapter.sol
src/vault-v2/adapters/CoinbasePrimeAdapter.sol
src/vault-v2/adapters/LotusV2Adapter.sol
src/vault-v2/adapters/VaultV2Adapter.sol
src/vault-v2/libraries/BaseLotusV2Adapter.sol
```

9 Post-Audit Solace Scan and Remediation Review

9.1 Overview

Following the two security audits, Cyfrin used Solace, its proprietary AI, to scan the specified deployment-candidate code on October 23, 2026.

Core-code and deployment-script remediations were reviewed at the single commit recorded below, which incorporates all of them. The scan scope and status counts are recorded separately from the two audits.

9.2 Review Details

Summary

Repository	lotus
Scan Date	October 23, 2026
Scan Commit	`cc62399d38e1e75d05e3a45f0cc6caec517af724`
Reviewed Remediation Commit	`4ad5fe3386a213175939fa5ed53bf943fbf4f5af`
Methods	Proprietary AI

Issues Found

Severity	Found	Resolved	Acknowledged	Pending
Medium Risk	7	4	3	0
Low Risk	14	3	11	0
Total	21	7	14	0

How to read the scan statuses

Resolved means Cyfrin reviewed the corresponding remediation at the reviewed remediation commit; it does not imply that a final deployment has been verified. Acknowledged means Lotus Labs chose to retain the reported behavior or accept the residual risk, as recorded in its response; this does not constitute resolution or endorsement by Cyfrin. Pending means an intended change has not been verified at the reviewed remediation commit. These categories are separate from the final audit statuses used elsewhere in this document.

9.3 Scan Scope

The Solace scan covered the following 86 files at the scan commit:

```
scripts/deploy/common/LotusGuardianPauseModule.sol
src/access/TwoStepOperator.sol
src/access/TwoStepOwnable.sol
src/bundler3/AdapterBase.sol
src/bundler3/ERC4626LotusBundlerAdapter.sol
src/bundler3/interfaces/IAdapterBase.sol
src/bundler3/interfaces/IERC4626LotusBundlerAdapter.sol
src/bundler3/interfaces/ILotusBundlerAdapter.sol
src/bundler3/LotusBundlerAdapter.sol
src/factories/interfaces/IModuleFactory.sol
src/factories/ModuleFactory.sol
src/governance/interfaces/ILotusGovernor.sol
```

src/governance/interfaces/IOperatorTimelock.sol
src/governance/LotusGovernor.sol
src/governance/OperatorTimelock.sol
src/hooks/interfaces/ILotusHooks.sol
src/hooks/libraries/Hooks.sol
src/interfaces/IBundler3.sol
src/interfaces/IERC20.sol
src/interfaces/IERC20Metadata.sol
src/interfaces/ILiquidationModule.sol
src/interfaces/ILotus.sol
src/interfaces/ILotusCallbacks.sol
src/interfaces/IOracle.sol
src/interfaces/IRiskEngine.sol
src/lens/interfaces/ILotusLens.sol
src/lens/LotusLens.sol
src/libraries/BaseUpgradeableModule.sol
src/libraries/ConstantsLib.sol
src/libraries/InterestMathLib.sol
src/libraries/LotusBalancesLib.sol
src/libraries/LotusErrorsLib.sol
src/libraries/LotusEventsLib.sol
src/libraries/LotusExternalLib.sol
src/libraries/MarketParamsLib.sol
src/libraries/PendingLib.sol
src/libraries/SharesMathLib.sol
src/libraries/UtilsLib.sol
src/liquidations/factories/HealthDiscountLiquidationModuleFactory.sol
src/liquidations/factories/OracleIncentiveLiquidationModuleFactory.sol
src/liquidations/HealthDiscountLiquidationModule.sol
src/liquidations/interfaces/IHealthDiscountLiquidationModule.sol
src/liquidations/interfaces/IHealthDiscountLiquidationModuleFactory.sol
src/liquidations/interfaces/IOracleIncentiveLiquidationModule.sol
src/liquidations/interfaces/IOracleIncentiveLiquidationModuleFactory.sol
src/liquidations/libraries/BaseLiquidationModule.sol
src/liquidations/libraries/LiquidationErrorsLib.sol
src/liquidations/OracleIncentiveLiquidationModule.sol
src/Lotus.sol
src/oracles/interfaces/AggregatorV3Interface.sol
src/oracles/interfaces/IBoundedStalenessFeed.sol
src/oracles/staleness/BoundedStalenessFeed.sol
src/risk-engines/factories/MonotonicManagedLinearKinkRiskEngineFactory.sol
src/risk-engines/interfaces/IBaseLinearKinkRiskEngine.sol
src/risk-engines/interfaces/IManagedLinearKinkRiskEngine.sol
src/risk-engines/interfaces/IMonotonicManagedLinearKinkRiskEngineFactory.sol
src/risk-engines/libraries/BaseLinearKinkRiskEngine.sol
src/risk-engines/libraries/BaseRiskEngine.sol
src/risk-engines/libraries/MonotonicUtilLib.sol
src/risk-engines/libraries/RiskEngineErrorsLib.sol
src/risk-engines/libraries/RiskEngineEventsLib.sol
src/risk-engines/ManagedLinearKinkRiskEngine.sol
src/risk-engines/MonotonicManagedLinearKinkRiskEngine.sol
src/vault-v2/adapters/CoinbasePrimeAdapter.sol
src/vault-v2/adapters/LotusV2Adapter.sol
src/vault-v2/adapters/VaultV2Adapter.sol
src/vault-v2/adapters/WGTXXAdapter.sol
src/vault-v2/factories/LotusVaultFactory.sol
src/vault-v2/gates/BinaryVaultGate.sol
src/vault-v2/interfaces/IAdapter.sol
src/vault-v2/interfaces/IAdapterRegistry.sol
src/vault-v2/interfaces/IBinaryVaultGate.sol
src/vault-v2/interfaces/ICoinbasePrimeAdapter.sol
src/vault-v2/interfaces/IERC20Skim.sol

```
src/vault-v2/interfaces/ILotusAdapterRegistry.sol
src/vault-v2/interfaces/ILotusV2Adapter.sol
src/vault-v2/interfaces/ILotusVaultFactory.sol
src/vault-v2/interfaces/ISettlementWindowGate.sol
src/vault-v2/interfaces/ISkimmable.sol
src/vault-v2/interfaces/IVaultV2.sol
src/vault-v2/interfaces/IVaultV2Adapter.sol
src/vault-v2/interfaces/IVaultV2Factory.sol
src/vault-v2/interfaces/IWGTXXAdapter.sol
src/vault-v2/libraries/BaseLotusV2Adapter.sol
src/vault-v2/libraries/Skimmable.sol
src/vault-v2/LotusAdapterRegistry.sol
```

Other deployment scripts were consulted as supporting context.

10 Attestation

Cyfrin attests that it performed two security reviews of the Lotus code provided by Lotus Labs.

The repositories, commits, review periods and combined finding counts with their final status are in Section 5. The individual audit sections record each engagement's scope and status counts. This attestation is limited to the documented scopes, audited commits and mitigations specifically reviewed by Cyfrin.

The subsequent Solace proprietary-AI scan and targeted remediation review are recorded separately in Section 9, with their own scope, commits and current statuses. That work is distinct from the two audits and does not verify deployed contracts or their on-chain configuration.

Cyfrin publishes this document and its SHA-256 hash at https://github.com/Cyfrin/cyfrin-audit-reports. To check a copy on macOS or Linux, run the following in the folder that contains it; it prints `OK` when the copy matches. If the copy was renamed, set F to its file name. Before running it, check that the URL is Cyfrin's repository.

```
U=https://github.com/Cyfrin/cyfrin-audit-reports/raw/main/reports/sha256
N=2026-11-12-cyfrin-lotus-v2.0.pdf
F=$N
H=$(curl -fsSL $U/$N.sha256 | cut -d' ' -f1)
echo "$H *$F" | shasum -a 256 -c
```

Cyfrin's full audit report with all findings provided to Lotus Labs has the SHA-256 hash and file name below. To check a copy of it, first check this document as above, then run the following in the folder that contains the full report; it prints `OK` when the copy matches. If the copy was renamed, set F to its file name.

```
H=c689b6dc776414e337915d0b4161f60e2e187247f64e1aadf3a3dbaf23242fd8
F=2026-11-12-cyfrin-lotus-v2.0-full.pdf
echo "$H *$F" | shasum -a 256 -c
```

On Linux, `sha256sum -c` can be used in place of `shasum -a 256 -c`. On Windows, run `Get-FileHash <file> -Algorithm SHA256` in PowerShell and compare the result with the hash.