Sherlock Bug Bounty Coverage Agreement

Details

Protocol Customer: Usual
Audit Report(s): Link
Maximum Desired Bug Bounty Payout Amount: 16,000,000 USDC
Maximum Desired Bug Bounty Coverage Amount: 500,000 USDC
Active Coverage Amount: The lesser of

1) Maximum Desired Bug Bounty Coverage Amount
2) 10% of the funds at risk

Coverage Provided for the Following Chain(s): Ethereum mainnet
Bug Bounty Coverage Amount: 100% of Active Coverage Amount
Exploit Coverage Amount: 0% of Active Coverage Amount
Bug Bounty Deductible: 15,500,000 USDC
Deductible Terms: If a payout exceeds the deductible, Sherlock/Nexus Mutual will pay 100% of the amount above 15,500,000 USDC up to 16,000,000 USDC
Eligible Severities: Only Critical severity payouts are eligible for coverage. High, Medium, and other severities will not be eligible for any payout by Sherlock and/or Nexus Mutual.
Validating Bug Bounty Submissions: Protocol Customer has full discretion to validate or invalidate submissions. If a submission is validated and Sherlock and/or Nexus Mutual disagrees, the process described in “Claims Process” below may be utilized.
Claims to be paid in: USDC
Bug Bounty Program Link: Temporary link
Covered Contract(s):

Core Contracts[1]:

Proxy Address	Implementation Address	Contract Name
0x73A15FeD60Bf67631dC6cd7Bc5B6e8da8190aCF5	0xae12f6f805842e6dafe71a6d2b41b28ba5fc821e	USD0
0x35D8949372D46B7a3D5A56006AE77B215fc69bC0	0xe025d17562a62159e6731298c5a51ad444529354	USD0PP
0xde6e1F680C4816446C8D515989E2358636A38b04	0x0eec861d49f15f585d6bb4301fc4f89bce22af4e	DaoCollateral
0x0D374775E962c3608B8F0A4b8B10567DF739bb56	0x7d355d14b8de1210ac69ebe3aebcc5e002cdf63b	RegistryAccess
0x0594cb5ca47eFE1Ff25C7B8B43E221683B4Db34c	0x81221180b4b2fc01975817d4b7e1f4adadcf8388	RegistryContract
0xB969B0d14F7682bAF37ba7c364b351B830a812B2	0xf65b0c88f65d620ea325ffb1ad46a5ba8a6e57d3	SwapperEngine
0xb97e163cE6A8296F36112b042891CFe1E23C35BF	0xdec568b8b19ba18af4f48863ef096a383c0ed8fd	ClassicalOracle
0x43882C864a406D55411b8C166bCA604709fDF624	0x334b18e5e81657efa2057f80e19b8e81f0e5783c	TokenMapping

Additional Contracts:

Proxy Address	Implementation Address	Contract Name
0xC4441c2BE5d8fA8126822B9929CA0b81Ea0DE38E	0x2b65f9d2e4b84a2df6ff0525741b75d1276a9c2f	Usual.sol
N/A	0xe1DeE60c516a8350704Ec24a6E856c9F533d1c1b	EulerOracle
0x75cC0C0DDD2Ccafe6EC415bE686267588011E36A	0xd004c92e2590b08a7684259007962e3db5d23dde	DistributionModule
0x58073531a2809744D1bF311D30FD76B27D662abB	0x88a6c0b3d3c006ba9bc189c08499b4d4e5062893	UsualUSDtb
0x4Cbc25559DbBD1272EC5B64c7b5F48a2405e6470	0xcdee8792f28e5c0713dc12c2bab8905ce24d44c1	UsualM
0x647F8987C288bf6D2fDb332918E1E14424839EDA	0x2792dad98fd6ba3743ca3484dbc2ce436faa9440	YieldModule
0x06B964d96f5dCF7Eae9d7C559B09EDCe244d4B8E	0x236ce5ed9e077ae63460148f860ed39d1b8808e9	UsualX
0x094B360AE512A65584d4f5Be33D68B2E08677b89	0x57e353c2e2d40f5b923512476a111127a6a21b63	UsualS
0xa55AF35E5F4bb6A82E0A290570BcE38Ce2757d37	0x24a2461f3e67e82930c2df2ab032e9272a272f65	UsualSP

Glossary

Active Coverage Amount - the maximum amount the Protocol Customer could be entitled to in the case of a successful claim
Commit - The commit hash in GitHub (or other code management software provider) which is the final group of changes made related to a Sherlock audit/fix review. The changes made in this commit hash must explicitly be signed off on by the Lead Senior Watson of the Sherlock audit. Any subsequent/additional commit hashes or deviations from the above process can result in voided coverage.

[1] Only vulnerabilities in Core Contracts are eligible for the Critical Severity tier and the maximum payout.

Current TVL - The total value locked in the Protocol Customer's Covered Contract(s) (as defined above).
Deductible - The amount the Protocol Customer must pay before Sherlock will contribute USDC to a claim. The deductible amount is always deducted from the Active Coverage Amount, meaning that if an Active Coverage Amount is $500k and the deductible is $50k, Sherlock can pay out a maximum of 450k USDC/DAI.
Maximum Desired Coverage Amount - The maximum desired amount of coverage that the Protocol Customer is willing to pay for. The Maximum Desired Coverage Amount is NOT necessarily the amount of funds owed to a Protocol Customer during a payout. Please refer to the Active Coverage Amount to determine the maximum amount the Protocol Customer could be entitled to for a successful claim.
Protocol Customer - The counterparty to this agreement, who has written/commissioned the code that was audited by Sherlock and whose coverage is now governed by this agreement
Protocol Code - The contract(s) listed under "Covered Contract(s)" above
Protocol Agent Address - The smart contract address provided to Sherlock, which is the address from which claims are made and from which a Protocol Customer's payout address can be changed
Staking Pool - The total value of all tokens (USDC, etc.) held in Sherlock's V2 staking pool
Token - Any cryptocurrency or form of value that exists on a blockchain (including NFTs, etc.)

Sherlock Coverage

If Sherlock has agreed to provide coverage on the Protocol Customer's Active Coverage Amount, this coverage will begin on the date the protocol has decided, provided all criteria in "Initiating and Maintaining Active Coverage" have been met.

Please see the section below, "The Spirit of Sherlock Exploit Protection", for a more detailed discussion around the types of smart contract and economic risks Sherlock intends to consider covered events.

In the event of a covered bug bounty submission or smart contract exploit, the Protocol Customer can submit a claim and be reimbursed up to the stated Active Coverage Amount minus the Deductible at the start block of the exploit. Only on-chain losses can be considered for exploit coverage and only direct bug bounty payouts can be considered for bug bounty coverage. Any bug bounty program hosted outside of Sherlock is not eligible for the coverage provided by Sherlock and/or Nexus Mutual. If for any reason the

affected user(s) or affected protocol(s) see a partial or full return of exploited funds before or after a payout from Sherlock, the returned funds must be deducted from the Sherlock payout and any amount paid out by Sherlock relating to the returned funds that had been lost (as part of a claim) must be returned to Sherlock. Please see the sections “Claim Validity”, “Sherlock Claims Process”, “Payment Process”, and “Deciding on Claims”, below for more detail.

Coverage Premium Pricing

Coverage premium pricing is communicated directly to the Protocol Customer by Sherlock. The amount necessary to keep coverage active can be found in the Sherlock Payment Portal for each Protocol Customer. Sherlock reserves the right to not provide coverage and refund any up-front coverage payments if the auditors and/or Sherlock don’t feel comfortable with the codebase after the audit has been completed.

Bug Bounty Coverage

At the completion of the audit, the Protocol Customer will implement a bug bounty program with a bounty valued at “Maximum Desired Bug Bounty Payout Amount” defined in the “Details” section on page 1 of this document. The program will be initiated through Sherlock’s Bug Bounty Platform. Bug bounty pricing is defined in “Details” at the top of this agreement.

A Bug Bounty Coverage payout may only occur if a bug bounty submission is validated by the Protocol Customer according to the rules of the Protocol Customer’s Bug Bounty Program, found in the Bug Bounty Program Link in the “Details” section on page 1. In the scenario where the Protocol Customer validates a bug bounty submission but Sherlock disagrees, Sherlock may utilize the process described in the “Claim Validity” section in order to determine if the coverage payout should be made.

Initiating and Maintaining Active Coverage

To initiate coverage, a Protocol Customer should send a deposit to Sherlock’s smart contract address defined in the “Payment Process” section, for at least 1 month's worth of payment.

The amount of the deposit that can be withdrawn by the Protocol Customer will continuously decrease while coverage is active. This is the premium amount a Protocol

Customer is “charged.” Sherlock updates the Protocol Customer’s Current TVL periodically to ensure the Protocol Customer doesn’t overpay for coverage.

In order to keep coverage active, the Protocol Customer will need to increase their balance in the Protocol Payment Portal if the “Active Balance” is less than 500 USDC or “Coverage Left” is less than 12 hours, as they run the risk of being temporarily removed from coverage. The coverage will end at the first block after the protocol is removed from coverage. For the avoidance of doubt, even if the Protocol Customer is not currently under coverage, a covered event that occurred during a block before the coverage ended could still be valid and Sherlock will properly assess and pay out that claim when relevant.

The Protocol Customer is advised against making material changes to the Protocol Code which have not been approved and audited by Sherlock. If the changes are approved, coverage will extend to the new contracts and Sherlock will follow up with a revised coverage agreement (this document), noting the new “Covered Contract(s)” in the section “Details”.

Sherlock will continue to provide active coverage on all contracts that were originally reviewed by Sherlock and deployed, even if a new unaudited contract(s) is added somewhere in the system. Basically, this just means that Sherlock is not “off the hook” on all the covered, audited contracts if the protocol deploys one incremental contract (or contracts) that has not been approved by Sherlock. Of course, the unapproved incremental contract(s) will not be under coverage and any exploit(s) that wouldn’t have been possible without this contract (or contracts) will not be covered.

In the event Sherlock does not review the new code changes and a bug bounty submission or exploit occurs, Sherlock’s two primary claims systems, the SPCC and UMA Optimistic Oracle (see section “Claim Validity” below), will be used to assess whether the attack vector would have happened regardless of the unaudited changes, or whether the attack vector was caused because of the unaudited changes. In the former situation, where the attack vector would have happened regardless, this could constitute a valid claim. In the latter situation, where the attack vector became possible because of the unaudited changes, this will not constitute a valid claim.

Payment Process

All initial Protocol Customer payments to Sherlock will be made in USDC to the following Ethereum smart contract address: 0x666B8EbFbF4D5f0CE56962a25635CfF563F13161.

After the initial coverage payment, subsequent payments should be made through Sherlock's Protocol Payment Portal.

Claim Validity

The Protocol Customer has full discretion to reject submissions and decide the amount that the Protocol Customer would like to pay for any submission.

Sherlock and Nexus Mutual may only pay out a claim that the Protocol Customer has deemed valid if Sherlock and Nexus Mutual originally agree on the validity and payout amount, or if the resolution process described below (the SPCC and Optimistic Oracle) decides that Sherlock and Nexus Mutual should make the payout.

If the Protocol Customer believes a submission should be paid out by Sherlock and/or Nexus Mutual but Sherlock and/or Nexus Mutual disagree, any party may push toward a resolution by first escalating the matter to the SPCC. The decision made by the SPCC will be binary (either a claim will be accepted or not) and it will be made in 7 days or less from the time the claim was submitted. Once a decision is made on a claim by the SPCC, there are a few possible paths. If the claim is denied by the SPCC, the first path for the escalating party is to accept the SPCC's denial and take no further action.

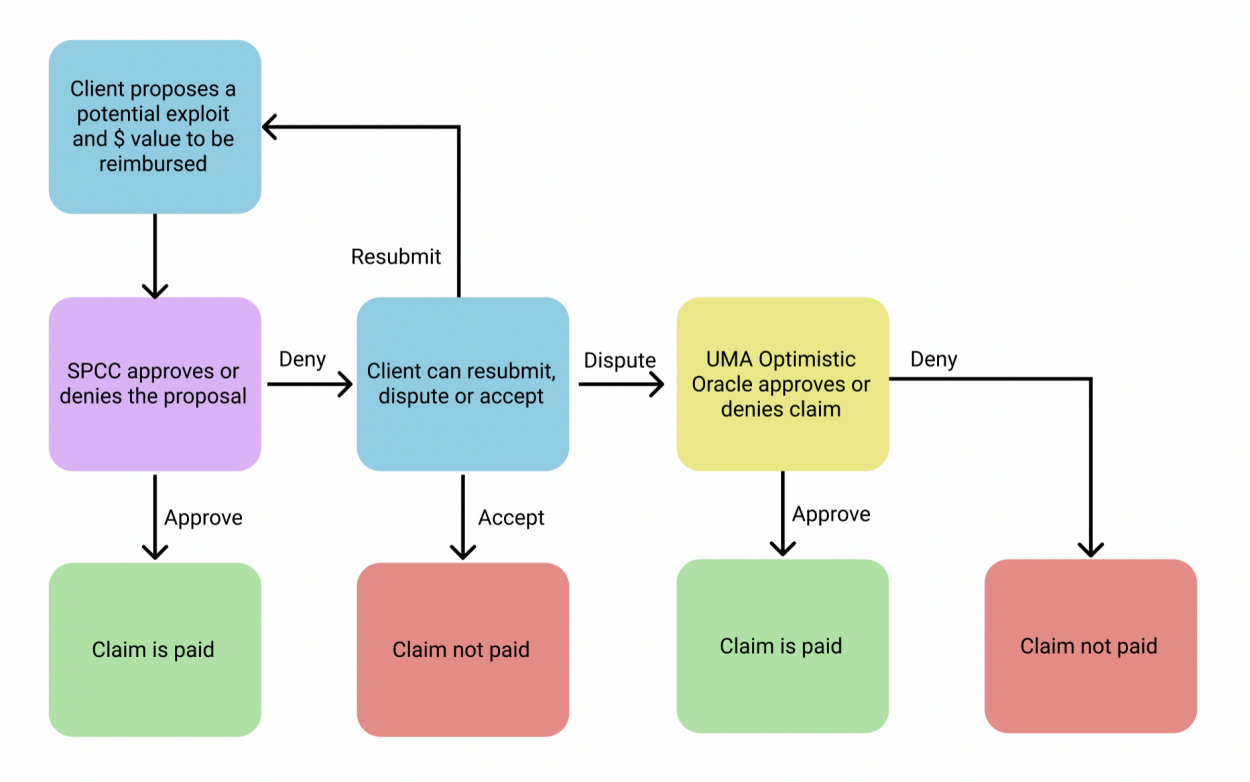
Note: If a Protocol Customer has an existing relationship with a member (or members) of the SPCC and that relationship could constitute a conflict of interest, the member (or members) are required to abstain from participating in any claim votes associated with the Protocol Customer.

The second path is to revise the claim (usually the amount of the claim) and re-submit. A submitter is limited to 3 submissions for each potential claim.

The third path is to escalate to arbitration further. This would require the partyl to "stake" the current fee charged by UMA to use their Optimistic Oracle (last priced at ~22k USDC). The escalation would move the claim decision from the SPCC's hands into the hands of UMA's Optimistic Oracle, more specifically UMA's Data Verification Mechanism. The escalating party will have 4 weeks to escalate the claim to UMA's Optimistic Oracle once it has been denied by the SPCC. When escalated to UMA's Optimistic Oracle, the claims decision will be voted on by UMA tokenholders and the resolution of that vote will be the final claim decision (overruling the SPCC).

If the escalating party is proven correct by the UMA Optimistic Oracle, then all parties agree to adhere to the decision. The escalating party will also receive their stake back, minus the fee charged by UMA for using the Optimistic Oracle. If the escalating party's escalation proves to be unsuccessful, then the stake is not returned. Further reading related to UMA's Optimistic Oracle and Data Verification Mechanism can be found here.

Visualization of Claims Process



Utilization of Coverage

Coverage Utilization

The Protocol Customer will be eligible to submit claims up to the Active Coverage Amount for a bug bounty or exploit that occurred at any time when they maintained active coverage (and kept a balance above 0 USDC). At any time, Sherlock may adjust the rate at which the premium will be calculated, although Sherlock endeavors to give (and has historically given) at least 2-weeks notice whenever a pricing change will go into effect.

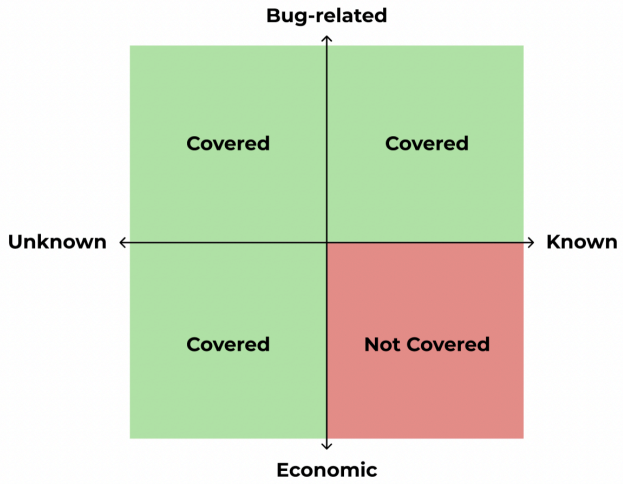
Whenever a claim is paid out by Sherlock to a Protocol Customer (including exploit, bug bounty payouts, etc.), that Protocol Customer is no longer considered to be under active coverage until the on-chain coverage is removed and a new agreement with Sherlock has been reached for new on-chain coverage.

Zero Balance Coverage

Technically, once a Protocol Customer's balance falls below 500 USDC or 12 hours worth of coverage, the covered protocol can be removed from coverage by anyone on-chain. Once a protocol is removed from coverage, they can no longer create claims for bug bounties or exploits that occurred on or after the timestamp at which they were removed from coverage. If a covered protocol's balance hits 0 USDC, the protocol's coverage is considered to be inactive, even if the protocol has not been technically removed from coverage in the smart contracts yet. A Protocol Customer would need to be removed and re-added to coverage at that point, they cannot simply replenish the balance once it gets to 0 USDC. If a protocol experiences a bug bounty submission or exploit during the time at which the protocol's balance is 0 USDC (or after an unauthorized replenishment has occurred), the event should not be paid out and the SPCC and UMA Optimistic Oracle should vote accordingly.

The Spirit of Sherlock Exploit Protection

This document will outline in detail all of the areas of coverage by Sherlock against which claims can be made (or not made). Because there are always bound to be gaps in explicit wording, Sherlock also attempts to explain the "spirit" of what the later paragraphs will convey, so that unforeseen attack vectors can still be handled well.



Known Economic Risks

There are two important categories of coverage at Sherlock. The first is bug-related coverage. If a smart contract has a syntax error or otherwise fails to execute its logic as intended due to a mistake related to code being written improperly, that would likely be considered a bug-related incident. However, if there is still a loss of funds despite the code being technically correct in what it

intended to do (as a third party would observe), this would likely fall more in the category of an economic incident. The latter (economic incidents) are not so much a failure of code or syntax as they are a failure of economic design. The difference can be subtle and there are definitely gray areas, but generally if the literal code functions in the way a developer intended (and in the way it was conveyed to Sherlock/auditors), that is likely an economic error. If the literal code does not function as intended, that is likely a bug-related error.

We can create a quadrant of coverage with four types of errors: unknown bug-related errors, known bug-related errors, unknown economic errors, and known economic errors. An unknown error is simply something that the developers/auditors are unaware of (until it surfaces). This means a common bug (in a known class of bugs) can still be an unknown bug in a specific contract because it was not identified in that contract. Whether a bug-related error was previously known or unknown, an incident related to a smart contract bug should generally be covered. The onus is on Sherlock's security team to find known bugs and help the Protocol Customer fix them securely. And unknown bugs are inherently unforeseeable so they should be covered.

For unknown economic risks, the sentiment is the same. Because it was unknown (and therefore unforeseeable), it should be covered.

But known economic risks are a bit different. Almost every protocol has some set of known economic risks. For example, if the value of Maker collateral falls below the value of the deposits made into the protocol, the depositors are at risk of losing funds. Same goes for almost anything related to token price volatility. If a token price goes down, holders of the token or parties who interact with that token are at risk of losing funds related to the price drop. These are examples of known economic risks. Sometimes, these risks are a large part of the reason APYs are so high for certain opportunities. These are not risks Sherlock intends to cover. Please see the "Specific Economic Events Not Covered By Sherlock" section below which includes some well-known economic risks for various protocol types.

Known Bug-Related Risks

If a Protocol Customer understands the implications of a known bug-related risk, but deems it an "acceptable risk" for their protocol (normally indicated with a "Won't Fix" or "Sponsor Disputed" label in a Sherlock audit repository), it is no longer considered to be covered by Sherlock.

If a Protocol Customer is warned/notified about a bug/vulnerability PRIOR to initiating coverage with Sherlock, this bug/vulnerability would not be considered covered by Sherlock. If the protocol that the Protocol Customer has forked has been notified publicly (or put out a notification) about a bug/vulnerability before the Protocol Customer initiated coverage this would also not be covered.

Sherlock attempts to enumerate, in as clear terms as possible, the events that will or will not be covered by Sherlock coverage:

Specific Economic Events NOT Covered by Sherlock

Token Price Fluctuations

Any loss of funds due to a change in token price or stablecoin depegging should almost certainly not be covered by Sherlock. Any protocol covered by Sherlock must know exactly which tokens it could have the opportunity to interact with (and will be audited based on this info). Any new token that a protocol intends to interact with should be treated just like any other new integration: with a security review by Sherlock before being executed on mainnet. And any protocol should have contingencies in their code for the price of all of these tokens dropping to zero or approaching infinity. The volatility of a token price is a perfect example of a “known economic risk” as recounted in the preceding section.

Changes in token price especially apply on the user side. The risk of a token’s price going down (or up in the case of short-selling) should always be considered a known risk and thus a loss of funds caused by a change in the price of a token alone should not be a claimable event.

Collateral Shortfalls (example: Lending Protocols)

This section is especially applicable to lending protocols and related protocols. Any lending protocol is well aware that one of the known economic risks is a shortfall in collateral, which would leave depositors unable to collect some or all of their principal. Of course, these collateral shortfalls could be caused by a bug in a smart contract, in which case Sherlock should cover the event. But a common, known economic risk of lending protocols is collateral shortfalls related to rapid and/or large changes in the price of tokens being used as collateral (or the oracles being relied upon for those token prices). This type of collateral shortfall would not be covered by Sherlock.

Unavailability of Funds (example: Lending Protocols)

This section is especially applicable to lending protocols and related protocols. There may be situations where a depositor's tokens are not available to be withdrawn due to high utilization (on the borrowing side) of the depositor's tokens. This is a known economic risk related to lending protocols and thus would not be covered.

Impermanent Loss (example: AMM Protocols)

This section is especially relevant for AMM-style protocols. Any LP in an AMM-style protocol should be aware of the risk of impermanent loss when providing liquidity to that protocol.

Slippage (example: AMM Protocols)

This section is especially relevant for AMM or exchange-style protocols. Any user who is doing transactions with an AMM or exchange-style protocol should be aware that losses due to slippage are possible. Slippage losses should generally not be covered by Sherlock.

Counterparty Risk (example: Undercollateralized Protocols)

This section is especially relevant for uncollateralized or undercollateralized lending protocols. If a counterparty or intermediary who received a loan does not repay the loan or has some other payment-related issue, this should not be covered by Sherlock.

Transaction Ordering Attacks / Frontrunning / Sandwich Attacks / MEV-Related Attacks / Chain Re-Orgs

Many of these types of attacks involve malicious addresses (usually controlled by bots) that spot profitable transactions in the mempool and then execute the transaction themselves in order to capture the profit. Or the malicious address sees a certain profitable state change that will be caused by a transaction in the mempool, and calls a function or executes a transaction to take advantage of that state change. Sherlock does not cover these types of attacks because they exist outside the bounds of the covered smart contracts. If a user gets front-run, it means that anyone in the world had a right to call the transaction that the user called, so the user did not necessarily have priority on the value gained from the transaction, which means the "loss" would not be covered.

However, in certain cases, related events would be covered by Sherlock. If, for example, a function was meant to be whitelisted but the modifier was missing, this could be covered because the Sherlock audit process should catch these types of bugs and it should be fairly clear that unsound logic was being used in the code. In other cases, it's not always

clear what the intentions of the developers were and therefore Sherlock cannot cover those cases.

Other Specific Events NOT Covered by Sherlock

Social Engineering

If a user is tricked or psychologically manipulated into performing an action or divulging confidential information that results in a loss of assets, Sherlock does not intend to provide reimbursement.

Approve Max / Approve Unlimited

The expectation for protocols covered by Sherlock is that they should discourage (or prevent) approving amounts (of tokens) to a contract above and beyond what is necessary for a specific transaction. Sometimes, it is not possible to entirely prevent this in the smart contracts, but it should at least be made impossible through the covered protocol's sponsored frontend/UI. Sherlock's goal is to protect end-users who may not be sophisticated users of crypto. Any user who goes against the recommendation of the sponsored UI and "approves unlimited" anyways can be thought of as a sophisticated user according to Sherlock. Users who approve more than they need for a specific transaction and then experience an exploit that drains funds held in their wallet (not at the covered protocol) will not be covered by Sherlock. To be clear, the user's funds that were in the protocol and lost due to an exploit would be reimbursed. Any funds taken from the user's wallet due to an excessively high approval value will not be reimbursed by Sherlock.

Rug Pulls / Admin Rights / Off-limits functionality

The unauthorized accessing of any function where access is white-listed or entirely disallowed is NOT covered (assuming the function's access control is properly implemented in the code). Sherlock strongly recommends multi-signature admin functionality for all accounts and admin contracts.

The risk of funds being lost in a single signature setup is too high for Sherlock to cover. And in a multi-signature setup, the preponderance of evidence related to a loss of funds points to a rug pull (or extremely poor key management), which is a situation Sherlock does not intend to cover. Therefore Sherlock cannot cover ANY "admin"-related attack vectors. Sherlock is not able to accurately assess these types of attack vectors currently and so the price of premiums would be far too high if these risks were covered by Sherlock. Sherlock is working to expand its coverage in this area. But for now, any attack

vectors related to privileged access (without an accompanying covered attack vector), will not be covered by Sherlock.

This also applies to any governance-induced loss of funds. If a majority of token holders decides to vote maliciously in any way, that cannot be covered. For example, if a majority of token holders decide to transfer a minority's share of tokens to themselves, this would not be covered. And if a malicious party somehow acquires enough tokens to make a malicious change through governance, this also should not be covered.

Note: A bug related to a missing (or incorrect) access control check (such as a missing modifier) would be covered. This is a mistake in the code, not a "rug pull" necessarily.

Contract / Admin Address Blocklisting / Blacklisting / Freezing

If a protocol's smart contracts or admin addresses get added to a "blocklist" and the functionality of the protocol is affected by this blocklist, Sherlock will not cover this. A specific example could be a USDC or USDT blocklist. If a protocol uses USDC but the protocol's contract addresses or admin addresses get blocklisted by USDC and the protocol can no longer function properly as a result, this should not be covered by Sherlock.

Mistakes in Deployment

If a vulnerability becomes possible due to a poorly executed deployment of smart contracts, this is not something Sherlock would cover. However, Sherlock can provide services to check the accuracy/effectiveness of a deployment. Right now, this is seen as an "add-on" to normal security services provided by Sherlock.

Phishing attacks

Users affected by phishing attacks related to their wallet (Metamask, etc.) would not be covered by a specific protocol's policy. Even if the tokens involved were tokens related to or distributed by a specific protocol that has a policy with Sherlock, this holds true.

Phishing attacks related to "fake" websites (i.e. websites hosted at domains other than the protocol's sponsored website/app) would also not be covered. The onus is on the user to ensure they are actually interacting with a covered protocol, not a duplicate, replica, or look-alike website or protocol.

Phishing attacks spawning from a covered protocol's sponsored website/app are also not covered (such as hijacking a DApp's DNS). Sherlock currently does not have the

resources to ensure and monitor the security of website / frontend-related vulnerabilities, but this may change in the future. If getting coverage for this kind of attack is a very high priority for a Protocol Customer, please reach out to Sherlock.

Front-end bugs

In the same vein as phishing attacks, Sherlock currently does not have the resources to ensure and monitor the security of website / frontend-related vulnerabilities, but this may change in the future. So Sherlock cannot cover any unintended loss of funds resulting from an attack vector in the frontend (defined as non-Solidity code or code that is not deployed on a blockchain) of a Protocol Customer. This means that code related to libraries like Web3.js or Ethers.js cannot be covered even if it is interacting with smart contracts. The code covered must be deployed on the covered blockchain and frontend code does not meet this criteria.

Keepers

If the protocol is set up in a way where it relies on “keepers” or some external address to execute a job or trigger an action, Sherlock will not be responsible for attack vectors/freezing/malfunctions caused by the action/inaction/misuse of the keeper by this party or a pause/bug in the blockchain itself. However, if the keeper’s code was in scope, reviewed and signed off on by Sherlock, then an attack vector becomes possible as a result of a bug in the keeper’s code (NOT the action or inaction of the party responsible for calling/maintaining the keeper), then, when taking into account the other facts of the situation, this could qualify as a covered attack vector.

Coverage of Layer 2, Sidechain, and Other Chain-Related Risk

Sherlock, unfortunately, cannot cover attack vectors caused by a bug in the blockchain/L2 code itself, but Sherlock does strive to help make protocols resilient against common scenarios (such as the chain freezing) experienced by blockchains during the audit phase.

Specific Events That Should Not Be Relied on for Decisions

Flash Loan

A flash loan by itself is simply a way to acquire more tokens. Any attack that can be accomplished with a flash loan can also be accomplished without a flash loan (by a whale, etc.). Therefore, the presence of a flash loan does not necessarily mean that an attack vector is covered. However, flash loans are often accompanied by other events

that can be considered covered attack vectors. If the flash loan is simply taking advantage of a known economic attack (liquidation may occur if a token price drops), then it would not be covered by Sherlock. The presence of flash loans by themselves in a potential attack vector is not a good indicator of whether an event should be covered or not.

Oracle Manipulations

Oracle manipulations are well-known events that have caused the loss of tokens in the past. Unfortunately, some oracles (a.k.a. price feeds) like Uniswap V3 are nearly impossible to perfectly protect against manipulation. The only way to protect a Uniswap V3 oracle against manipulation is for the Protocol Customer or Sherlock to LP a certain amount of funds in the pool, across the entire tick range, and never move them. Because Sherlock and most Protocol Customers are not able or willing to provide this liquidity, Uniswap V3 oracles must always be used "at your own risk." For this reason, Sherlock cannot cover oracle manipulations on Uniswap V3 price feeds or similar price feeds.

For a similar reason, off-chain oracle providers such as Chainlink are also not covered by Sherlock. Sherlock does not cover Protocol Customers against any oracle/price feed risks, such as stale prices, manipulated prices or other malfunctions. However, Sherlock does strive to point out areas during the audit where these risks can be mitigated/handled.

Specific Events Covered by Sherlock

Specific Known "Bug-related" Attacks

Note: All must result in a loss of funds. A temporary pause in the availability of funds (or losses caused by a temporary pause) would not be covered.

- Integer underflow/overflow
- Reentrancy including cross-function reentrancy
- Silent failing sends / unchecked sends / unchecked low-level calls / delegatecall to untrusted callee
- Unbound loops
- Self-destruct-related attack vectors / forcibly sending Ether to a contract
- Denial-of-service due to fallback function, gas limit reached, unexpected throw, unexpected kill
- False randomness / reliance on "private" information being sent through the mempool
- Time manipulation / timestamp dependence
- Short address attacks

- Insufficient gas griefing
- Authorization through tx.origin
- Uninitialized storage pointer
- Missing checks / callable initialization function
- Missing variables / using the wrong variable
- Proxy/upgradability-related attacks (such as the OpenZeppelin UUPS bug)
- External dependencies if they were in scope of the audit

Known "bug-related" attacks not listed here

The list of specific, known bug-related attacks above is surely incomplete, but is provided mainly for convenience. It is not an exhaustive list of attack vector types that Sherlock could pay out and just because an attack is not listed above doesn't mean that it couldn't be covered.

Events that Combine Different Attacks

Many attack vectors combine multiple types of events. As long as just one of the events in the combined attack is determined to be covered by Sherlock, then the attack could be covered. In the opposite direction, if one or more of the events in the combined attack is explicitly not covered, it doesn't mean that the aggregated attack couldn't be covered. Losses due specifically to uncovered events always remain uncovered, even in the event of being combined with an incident involving a covered event.

Composability

Sherlock recognizes that composability and a protocol's need to integrate with other projects is a valuable part of the DeFi ecosystem. However, for the security of Sherlock's staking pool, and consequently its covered customers, Sherlock needs to take a careful approach to how integrations are covered.

Both extremes seem unrealistic to expect. It's unreasonable to *only* cover integrations that are done with protocols previously audited by Sherlock. However, it's equally unreasonable to expect Sherlock to cover an integration with any protocol under the sun. So, Sherlock is taking an incremental approach, where the covered integrations will include a whitelisted set of protocols, as well as any protocol whose code has been previously audited by Sherlock (but only the contracts in scope of the Sherlock audit and at the commit hash Sherlock signed off on). Of course, the Protocol Customer still needs to have the integration code go through Sherlock's full audit + fix review + coverage process.

The current list (which will update as Sherlock adds more protocols to coverage) can be found here:
https://github.com/sherlock-protocol/integrations-whitelist/commit/b343edd5d6d1f44e11abfc75c63240c6fc546081

If there is an attack vector present and a covered integration also has coverage from Sherlock or another coverage provider, and a payout takes place (or is scheduled to take place) for that integrated protocol, and the Protocol Customer receives reimbursement from that payout, then the total amount possible to be paid out to the Protocol Customer will be netted against the first payout. This is to ensure that Sherlock doesn't pay the same affected party more than their loss amount.

Let's say a Sherlock-covered protocol integrates with ACME Protocol. If ACME Protocol upgrades their code and it creates the potential for an exploit in the Sherlock-covered protocol, this will NOT be under coverage because the code of the integrating protocol changed from the time at which an audit for the Sherlock-covered protocol took place, meaning it would have been difficult for Sherlock to protect against this.

Attack Vectors Specific to Usual

Any issues found in the audit report which were acknowledged by the Protocol Customer, or not fixed, will be excluded from coverage.

Other specific attack vectors for the protocol include:
N/A

This coverage agreement and any associated addendums (whitelisted protocol list, bug bounty description) constitute the entire coverage terms and no participant, or Sherlock as a whole, shall be liable in any manner by any warranties, representations or covenants outside this coverage agreement wording.