All Participants October 22, 2026 at 7:40 pm

TIntervention (Immunefi)

Hi all,

We are concluding the mediation on this report, and we are setting out Immunefi's determination below as the record.

The impact

The report identifies two defects in the market contract's supply withdrawal path. The finalize callback runs on a fixed 8 TGas budget regardless of how many entries were processed, so when it fails the outer receipt's state changes persist and leave supply positions with `outgoing` greater than zero and `active` at zero. Those positions can re-enter the queue, because `Deposit::total()` includes `outgoing`. When the queue processes them, `record_withdrawal_initial` returns `WithdrawalAttempt::EmptyPosition`, the entry is removed without being added to the batch, and the loop's only exit condition is never satisfied. The receipt then terminates on NEAR's per-receipt storage-proof limit and every removal reverts, restoring the queue intact. Templar Protocol confirmed this mechanism on October 2nd.

Severity

The report results in the Critical impact "Permanent freezing of funds" on the impacts in scope table at the time of escalation.

On `ibtc-iethusdc-1.v1.tmplr.near`, which retained a full-access key, the freeze is recoverable by deploying replacement code, and on that market alone the impact would be "Temporary freezing of funds". On `ixlm-ixlmusdc.v1.tmplr.near` it is not. That market is deployed under the `v1.tmplr.near` registry and is not one of the two older markets the program excludes by name. It runs v1.2.0, which carries the same fixed-gas finalize callback and the same `EmptyPosition` branch as v1.3.0. It held one access key in its history, a full-access key deleted in transaction 5PPCjn583spZKptMEo1gYN4zuhCRhnWKwsTKxag3FQFd on January 19th, which is 114 days before submission, and no access key has existed since. The market contract has no admin, upgrade or pause method. For a supplier the withdrawal queue is the only way borrow-asset tokens leave the market, since `harvest_yield` credits the supply record without transferring out and `cancel_supply_withdrawal_request` removes only the caller's own entry. The queue is processed from the front, and the wall cannot be cleared in parts, because empty positions do not increment the batch count and the receipt reverts every removal regardless of the `batch_limit` passed. So on that market

no party other than the attacker can restore withdrawals, and the freeze is permanent. The most severe applicable impact governs the report.

Griefing

The "When Is An Impactful Attack Downgraded To Griefing?" article (https://immunefisupport.zendesk.com/hc/en-us/articles/17455102268305-When-Is-An-Impactful-Attack-Downgraded-To-Griefing) does not apply. Where a freeze is temporary and principal is returned in full, the damage is the delayed access, and Templar Protocol's measure on that basis was correct. That measure depends on recovery within a bounded period. On a market with no access key there is no recovery at any duration, the principal is not returned, and the principal is the damage.

Certora L-05 and the Previous Audits clause

The program provides that any unfixed vulnerabilities mentioned in Templar Protocol's published audit reports are not eligible for a reward. The vulnerability in this report is not mentioned in them.

Certora's manual review ran from August 25th to September 19th, 2025, against review commit a96e44d, with a final commit at 08d32ef. At a96e44d, and at 312d1c7a on September 21st, 2025, `execute_next_supply_withdrawal_request` takes no arguments and there is no `batch_limit`, no batch loop and no `EmptyPosition` branch. Both appear first in ac072f1f on October 29th, 2025, forty days after the review window closed. L-05 is marked Acknowledged, so it was not revisited in a fix-verification pass. L-05's own text describes the queue as processed by manual execution of each request, which is the pre-batch architecture. Its defect is a configurable minimum set very low or to zero, its stated harm is that legitimate withdrawals are significantly delayed, and its recommendation is to enforce reasonable minimum withdrawal amounts during market configuration. The entries it describes are processable and the queue drains. The entries here are not processable and the queue does not drain. The affected markets run a configured minimum of 400000 rather than zero, and a ghost entry re-queues at an amount that has already satisfied that check, so raising the minimum would raise the cost per account rather than prevent the wall. Templar Protocol's fix commit dbfcd42b changes the loop to count entries visited rather than requests fulfilled and scales the finalize callback's gas with the batch size, which are the two defects in this report and are not a minimum.

Guvenkaya GUV-1 and Thesis Defense findings 8 and 12 were reviewed at commits aeb8a93d and 4cdab4e7, which also predate the batch logic.

The Sybil exclusion

The program places impacts from Sybil attacks out of scope. That exclusion does not reach this report. A Sybil attack subverts a system that relies on distinct identities. This market relies on no such assumption, and one queue entry per account is a data structure rather than an identity control. Each attacker account satisfied the configured minimum with a real deposit, paid its own storage and account creation, and received exactly the one entry it paid for. The account count sizes the wall, and the impact comes from the contract's execution path. The exclusion sits alongside 51% attacks, lack of liquidity and centralization risks, which operate against correctly implemented code. A reading broad enough to exclude this report would also exclude the scenario described in Certora L-05 and the "Unbounded gas consumption" impact on the program's own impacts in scope table.

Proof of Concept

The proof of concept submitted on May 13th relied on a 300 TGas transaction limit that was no longer in force on mainnet at that date, and we said so to the security researcher on September 28th. The defect identified in that report is unchanged, being the fixed-gas finalize callback, the resulting positions, and the `EmptyPosition` branch that removes an entry without incrementing the batch count. What changed is which protocol limit stops the call. The demonstration of September 30th shows the impact against the deployed state of `ixlm-ixlmusdc.v1.tmplr.near`, and satisfies the Proof of Concept Guidelines and Rules (https://immunefisupport.zendesk.com/hc/en-us/articles/9946217628561-Proof-of-Concept-PoC-Guidelines-and-Rules).

Reward

Under the program, the Critical reward is 10% of the funds directly affected, calculated at the time and date the report was submitted, with a minimum of USD 50,000 and a maximum of USD 100,000. The supply on `ixlm-ixlmusdc.v1.tmplr.near` at submission exceeds USD 1,000,000, so the calculation reaches the maximum and the reward under the program is USD 100,000. The Repeatable Attack Limitations reach the same figure, since the contract can be neither upgraded nor paused.

Templar Protocol has offered USD 2,500 as a goodwill payment, which the security researcher has declined. The security researcher is open to discussing the amount if Templar Protocol wishes to engage, and any figure would come back to the security researcher before anything is conveyed. Immunefi holds no funds for any program, and payment is made by the project directly.

A safety note from the security researcher

Passed on at the security researcher's request, and separate from the severity and payout discussion. The legacy market `ixlm-ixlmusdc.v1.tmplr.near` still holds approximately USD 59,000 of supplier funds (block 219400038, `deposited_active` 591379738191 at 7 decimals) on code with no access keys, so it cannot be patched. The security researcher asks that remaining suppliers be told to withdraw or migrate while the queue is still healthy.

Corrections to our own earlier positions

Our message of September 25th stated that the report results in "Temporary freezing of funds", and our message of September 28th stated that it results in "Unbounded gas consumption". Both addressed only `ibtc-iethusdc-1.v1.tmplr.near`. Our message of September 30th accepted that the freeze is recoverable, which is true of that market and not of `ixlm-ixlmusdc.v1.tmplr.near`. Our message of September 30th also stated that the griefing ratio test does not apply because the freeze does not resolve on its own, and Templar Protocol correctly identified that reasoning as wrong, which we withdrew on October 6th. Our message of October 6th stated that we had reviewed both audit reports in the audits folder when the folder held three, and we had not then read the Certora report. We are sorry for those errors.

Publication

This program adheres to Responsible Publication Category 2, Notice Required (https://immunefi.com/responsible-publication/). The mediation concludes with this message, and the security researcher's rights under that policy apply accordingly.

Immunefi Mediation Team

1. Reported | 2. Escalated | 3. Confirmed | 4. Paid HIDE DETAILS

Your submission has been escalated to Templar Protocol.

WHAT'S NEXT?

After Templar Protocol reviews your submission, they'll follow up with a decision or request more information. In the meantime, if you discover any additional