AUDITONE

Audit Report

AURORA

09.05.2023

Table of Contents

CONTENTS

INTRODUCTION

Smart Contract Security Analysis Report

Note: This report may contain sensitive information on potential vulnerabilities and exploitation methods. This must be referred internally and should be only made available to the public after issues are resolved (to be confirmed prior by the client and AuditOne).

INTRODUCTION

Csanuragjain, Defsec, Cryptoninja and Ubermensch, who are auditors at AuditOne, successfully audited the smart contracts (as indicated below) of Aurorafastbridge. The audit has been performed using manual analysis. This report presents all the findings regarding the audit performed on the customer's smart contracts. The report outlines how potential security risks are evaluated. Recommendations on quality assurance and security standards are provided in the report.

01-PROJECT DESCRIPTION

The Aurora environment consists of the Aurora Engine, a high performance EVM—Ethereum Virtual Machine—and the Rainbow Bridge, facilitating trustless transfer of ETH and ERC-20 tokens between Ethereum and Aurora, within a great user experience.

Aurora exists and is operated as an independent, self-funded initiative, but will continue to leverage the shared team DNA and continually evolving technology of the NEAR Protocol.

The governance of Aurora will take a hybrid form of a Decentralized Autonomous Organization—the AuroraDAO—complemented by a traditional entity which will hold one of several seats in the AuroraDAO.

This audit focused on the Fast Bridge, one-way semi-decentralized bridge created to speed up transfers from Near to Ethereum.

02-Project and Audit Information

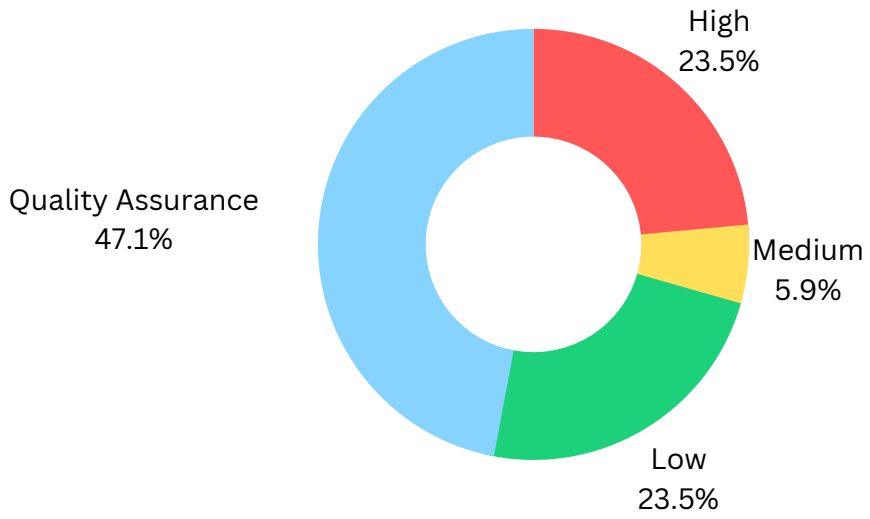
Term	Description
Auditor	Csanuragjain, Defsec, Cryptoninja and Ubermensch
Reviewed by	Gracious
Type	Bridge
Language	Rust
Ecosystem	NEAR and Ethereum networks
Methods	Manual Review
Repository	https://github.com/aurora-is-near/fast-bridge-protocol/
Commit hash (at audit start)	2c372fc90706a8ac192de2709d017c6431a7f0f6
Commit hash (after resolution)	d05f29fc8bf2bfe5eff83c47233fcc90ebb86891
Documentation	[Added once the whitepaper is published by the project]
Website	https://aurora.dev/
Submission Time	01-03-2023
Finishing Time	09-05-2023

03-Contracts in Scope

- fast-bridge-protocol/near/contracts/bridge/src/lib.rs
- fast-bridge-protocol/near/contracts/bridge/src/lp_relayer.rs
- fast-bridge-protocol/near/contracts/bridge/src/whitelist.rs
- fast-bridge-protocol/near/contracts/bridge/src/ft.rs
- fast-bridge-protocol/near/contracts/bridge/src/utils.rs

04-Executive summary

Aurorafastbridge plugin's smart contracts were audited between 2022-12-06 and 2023-03-14 by Csanuragjain, Defsec, Cryptoninja and Ubermensch. Manual analysis was carried out on the code base provided by the client. The following findings were reported to the client. For more details, refer to the findings section of the report.



Issue Category	Issues Found	Resolved	Acknowledged
High	4	4	0
Medium	1	1	0
Low	4	4	0
Quality Assurance	8	8	0

05-Severity Definitions

Risk factor matrix	Low	Medium	High
Occasional	L	M	H
Probable	L	M	H
Frequent	M	H	H

High: Funds or control of the contracts might be compromised directly. Data could be manipulated. We recommend fixing high issues with priority as they can lead to severe losses.

Medium: The impact of medium issues is less critical than high but still probable with considerable damage. The protocol or its availability could be impacted or leak value with a hypothetical attack path with stated assumptions.

Low: Low issues impose a small risk on the project. Although the impact is not estimated to be significant, we recommend fixing them on a long-term horizon. Assets are not at risk: state handling, function incorrect as to spec, issues with comments.

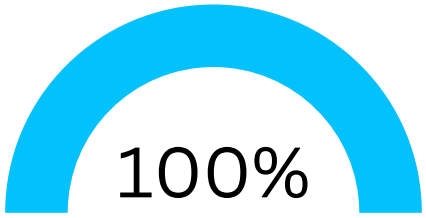
Quality Assurance: Informational and Optimization - Depending on the chain, performance issues can lead to slower execution or higher gas fees. For example, code style, clarity, syntax, versioning, off-chain monitoring (events, etc.)

Occasional: This category might represent risks with a moderate chance of occurring. These risks are not common but have happened in similar situations.

Probable: This category represents risks that are likely to happen. There's a high probability based on past experiences, current conditions, or future projections.

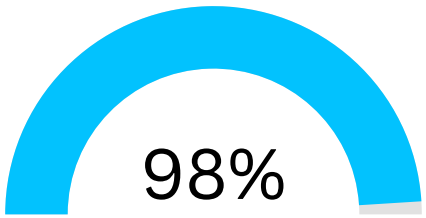
Frequent: This category represents risks that occur regularly. In a security audit, this might refer to common vulnerabilities or threats consistently observed in similar systems or environments.

06-Audit Overview



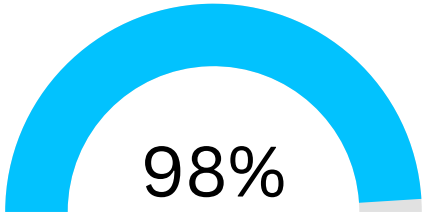
Security score

Security score is a numerical value generated based on the vulnerabilities in smart contracts. The score indicates the contract's security level and a higher score implies a lower risk of vulnerability.



Code quality

Code quality refers to adherence to standard practices, guidelines, and conventions when writing computer code. A high-quality codebase is easy to understand, maintain, and extend, while a low-quality codebase is hard to read and modify.



Documentation quality

Documentation quality refers to the accuracy, completeness, and clarity of the documentation accompanying the code. High-quality documentation helps auditors to understand business logic in code well, while low-quality documentation can lead to confusion and mistakes.

07-Findings

Finding: #1

Issue: Block Reorg Can Allow For Double Spending

Severity: High

Where: Business logic

Impact: Block reorgs can harm the protocol's logic by invalidating previously confirmed transactions. For example, if a transaction is included in a block that is later reorganized, the transaction may no longer be valid. This can lead to double-spending or other issues if the transaction was used to transfer tokens or execute a smart contract function.

In the case of the Fast Bridge project, block reorgs can cause problems if they occur during the transfer of tokens between Ethereum and NEAR. Specifically, if a block reorg occurs after the tokens have been locked on one chain but before they are unlocked on the other chain, the tokens may be lost or double-spent. This can happen because the LP-Relayer may have already released the tokens on the other chain, assuming that the transaction was confirmed, but the reorg means that the transaction is no longer valid.

Description: Block reorg, also known as blockchain reorganization, is a situation where a competing chain replaces the main blockchain. This can happen when multiple miners find valid blocks at the same time, and the network has to decide which block to include in the blockchain. In some cases, the network may choose to include a block that is not in the main blockchain, resulting in a reorganization of the chain.

Recommendations:
To mitigate the risk of block reorgs, the Fast Bridge project may need to implement additional measures, such as waiting for multiple confirmations before proceeding with token transfers or implementing a fallback mechanism in case of a block reorg.

Status: Resolved. Double spending is no longer possible because the Near side requires proof of nonexistence transfer, the Eth side relayer passes **valid_till_block_height** to the **transfe**r function, and proof verifications and block height are done only on finalized blocks on the Near side.

Finding: #2

Issue: Potential for Race Condition between Unlock Time and Proof Verification leading to Double Spending

Severity: High

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/master/src/transfer.rs

Impact: If there is a race condition, it means that the **LP-Relayer** may release the tokens before the proof of transaction has been fully verified. This can happen if the **LP-Relayer** is attempting to double spend the tokens, or if they are hacked or compromised and someone else is trying to steal the tokens.
If the **LP-Relayer** releases the tokens before the proof of transaction has been fully verified, then the sender's tokens will be unlocked on the NEAR side, and they will be able to spend them again. This means that there is a potential for double spending, as the **LP-Relayer** can then use the same tokens to make another transaction.

Description: In the Fast Bridge project, a race condition between unlock time and proof verification can lead to double spending. Here's how it can happen:
When a user sends tokens from Ethereum to NEAR, the tokens are locked on the Ethereum side, and the **LP-Relayer** is responsible for releasing the tokens on the NEAR side once the proof of transaction has been received. The **LP-Relayer** has a specific time window in which to release the tokens, which is set by the sender when they initiate the transaction.

Recommendations:
To prevent this from happening, it's important that the **LP-Relayer** is trusted and secure, and that there are appropriate measures in place to verify that the proof of transaction is valid before the tokens are released. This can include using secure verification processes, and having multiple parties involved in verifying the proof before the tokens are released.

Status: Resolved. Double spending is no longer possible because the Near side requires proof of non-existent transfer, the Ethereum's side relayer passes valid_till_block_height to the transfer function, and proof verifications are done only on finalized blocks on the Near side

Finding: #3

Issue: User can drain all funds by calling withdraw multiple times

Severity: High

Where: https://github.com/aurora-is-near/fast-bridge-protocol/blob/master/near/contracts/bridge/src/lib.rs#L628-L668

Impact: Attacker can withdraw more than his actual balance

Description: Currently **withdraw** function transfer tokens and after its success, the **callback** function decreases user's balance. A malicious user could call the **withdraw** function repeatedly before the **callback** function is called, as the main call and callback handler are independent transactions. This is because the user's balance is not decreased until the **callback** function is called, so the user can still transfer tokens.
However, the team already had **ACL and whitelisting functionality** (limited to Aurora), so no users could have been affected at that time.

Recommendations:

- It is recommended to follow CEI pattern in this case.
- Also **decrease_balance** should be moved to **withdraw**, above **ft_transfer**.

Status: Resolved. Project team followed CEI pattern, and moved **decrease_balance** to **withdraw**, above **ft_transfer**.

Finding: #4

Issue: Malicious user can double-unlock his locked funds

Severity: High

Where: https://github.com/aurora-is-near/fast-bridge-protocol/blob/master/near/contracts/bridge/src/lib.rs#L352-L396

Impact: Loss of funds. Wrong deductions of **pending_transfers_balances.**

Description: Currently **unlock** function checks whether pending transfer of the nonce does exist or not, after its success, the callback function increases balance and remove transfer.
In Near, main call and callback handler are independent transaction, so a malicious user can call unlock repeatedly, before callback function finished.
As pending transfer is not removed yet, user can still pass the check in second call.
Second call of **remove_transfer** in callback will not panic but only return None.
As a result, user can double-unlock his funds.
However, the team already had **ACL and whitelisting functionality** (limited to Aurora), so no users could have been affected at that time.

Recommendations: We should check if the **nonce** still exists in the **pending_transfers** at **unlock_callback**.

Status: Resolved. A check was added to determine if the **nonce** still exists in the **pending_transfers** at **unlock_callback.**

Finding: #5

Issue: Subscribed message may get lost

Severity: Medium

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/master/src/async_redis_wrapper.rs#L148-L150

Impact: If an error occurs while sending the received event message, then this event would get lost and would not be processed

Description:

- The **subscribe** function will stop if there is any error while sending the **pubsub_msg**.
- Restarting the **subscribe** function may take time
- Within that time all published events would get lost and wont be processed.

Recommendations:
Probably an offchain component can keep track of all lost event messages and Admin could send those lost event messages so that they could be processed

Status: This was resolved using one of the following approaches:

- Use Redis streams instead of basic Pub/Sub;
- Just scan events for a given block range to ensure no events are lost.

Finding: #6

Issue: Lack of Validation for **valid_till_block_height** on FastBridge Service

Severity: Low

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/5ed18302ae675e849e0f34b955f0646028946406/src/event_processor.rs

Impact: With the correct validation in place, FastBridge Service can ensure that transactions are executed within the specified **valid_till_block_height**, reducing delays and enhancing efficiency.

Description: The FastBridge Service, which is responsible for managing transfers between the NEAR and Ethereum networks, does not validate the **valid_till_block_height** parameter. This parameter is used to set an expiration block height for the transfer, and if not validated properly, it could result in transfers being processed after they have expired.

Recommendations: To address this issue, it is recommended that the FastBridge Service implement proper validation for the **valid_till_block_height** parameter. This could include checks to ensure that the current block height is not greater than the **valid_till_block_height** value.

Status: This was resolved by implementing proper validation for the **valid_till_block_height** parameter.

Finding: #7

Issue: Redis db connection issue - Relayer fund loss

Severity: Low

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/master/src/event_processor.rs#L71

Impact: If transaction was executed on ethereum meaning token were transferred but due to connection issue redis db was not updated then user can unlock near token as well

Description:

- User A uses fast bridge to get token on ETH
- Relayer executes the transaction on ETH but due to redis issue, the **PENDING_TRANSACTIONS** entry could not be made in Redis
- This causes Relayer to be unaware about this issue and Relayer now wont issue **lp_unlock** on near side
- After bridge request expire user can unlock the token. This means user gets both token on eth and near side

Recommendations: Revert if redis connection issue is present

Status: Resolved. This won't happen anymore, as **state proofs** are being utilized for **unlock()**. This means the user will need to provide proof of the non-existence of the transfer on the Ethereum side. Thus, he would be able to unlock it only if the transfer on Ethereum didn't happen.

Finding: #8

Issue: Missing comparison between **lock_time_min** and **lock_time_max** in **set_lock_time** function

Severity: Low

Where: https://github.com/aurora-is-near/fast-bridge-protocol/blob/master/near/contracts/bridge/src/lib.rs

Impact: Without checking the relationship between **lock_time_min** and **lock_time_max**, the code might allow an invalid configuration state that could lead to unexpected behavior or runtime errors in other parts of the application that rely on the lock duration.

Description: In the **set_lock_time** function, the **lock_time_min** and **lock_time_max** values are not compared before setting the **lock_duration**. This might lead to a situation where **lock_time_min** is greater than **lock_time_max**, which could be an invalid state for the intended logic of the application.

Recommendation: To prevent potential issues with invalid lock duration configurations, we recommend adding a comparison between **lock_time_min** and **lock_time_max** before updating the **lock_duration**. If **lock_time_min** is greater than **lock_time_max**, the function should return an error or panic to indicate that the provided values are invalid.

Status: This was resolved by adding a comparison between **lock_time_min** and **lock_time_max** before updating the **lock_duration.**

Finding: #9

Issue: Lack of Check for Same **token_eth** and **recipient** in the NEAR Contract

Severity: Low

Where: https://github.com/aurora-is-near/fast-bridge-protocol/blob/master/near/contracts/bridge/src/lib.rs

Impact: If the **token_eth** and **recipient** fields are the same, the contract might execute transfers that are not intended or logically incorrect, leading to unexpected outcomes and inaccurate records.

Description: In the provided code snippet, a JSON object is created, containing the details for a transfer, including the **token_eth** and **recipient** fields. However, there is no check to ensure that the **token_eth** and **recipient** fields are not the same. Allowing the same value for both fields could lead to potential issues in the contract's execution, as it might not be the intended behavior for a valid transfer.

Recommendations: To address this issue, it is recommended that the NEAR contract includes a check to ensure that the **token_eth** and **recipient** fields are not the same.

Status: This was resolved by adding a check to ensure that the **token_eth** and **recipient** fields are different.

Finding: #10

Issue: Missing comments on Code

Severity: Quality Assurance

Where: Almost all contracts

Impact: Lack of comments make it harder to understand what a specific function is doing.

Description: Most of the contract functions are missing comments.

Recommendations: Recommended to add comments on all contract functions.

Status: Resolved. Comments were added to all necessary functions.

Finding: #11

Issue: Unexpected token unlock could happen

Severity: Quality Assurance

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/master/src/transfer.rs#L115-L124

Impact: Token will get unlocked before User expectation causing transfer to not work. User will need to again start the transfer using only **valid_till** argument, wasting gas and time of user.

Description:

- As per docs, max of **valid_till** or **valid_till_block_height** is always taken to derive the unlock time:
  "**valid_till_block_height: Option<u64> — the same as valid_till, but in block height, not in nanoseconds. If both values are provided, tokens will be locked on the max of the two values. (In that stage for User only None value makes sense)**".
- But seems like **valid_till_block_height** is not actually used while checking valid time validity
- As we can see in below function unlock time validation is only performed on **valid_till** parameter and **valid_till_block_height** param is not used.

Recommendations: **valid_till_block_height** should also be used to derive the unlock time.

Status: This issue was resolved by using **valid_till_block_height** to derive the unlock time.

Finding: #12

Issue: Improve handling of **CheckToken** case in **check_whitelist_token_and_account** function

Severity: Quality Assurance

Where: https://github.com/aurora-is-near/fast-bridge-protocol/blob/master/near/contracts/bridge/src/whitelist.rs

Impact: The current implementation with an empty block might lead to confusion for developers who are reading or maintaining the code. They might not understand the purpose of the **CheckToken** variant and why there is no action associated with it. This could potentially lead to future bugs or unnecessary code modifications.

Description: In the **check_whitelist_token_and_account** function, the **CheckToken** variant of the **WhitelistMode** enum has an empty block, which might be unclear to readers of the code. This variant is intended to indicate that only the token needs to be checked against the whitelist, and no action is required for the associated account. However, the current implementation with an empty block might not effectively communicate this intent.

Recommendations: To improve the clarity and maintainability of the code, we recommend using the **_ => {}** pattern in the match statement for the **CheckToken** variant. This pattern makes it explicit that no action is needed for this case. Alternatively, you can add a comment within the empty block to explain why no action is required.

Status: Resolved by using the **_ => {}** pattern in the match statement for the **CheckToken** variant.

Finding: #13

Issue: Unnecessary Initialization verification

Severity: Quality Assurance

Where:
fast-bridge-protocol\near\contracts\bridge\src\lib.rs

Impact: This redundancy in the code can lead to gas wastage and possibly cause confusion for future developers who may not understand the reason for the additional check.

Description: The **require!** statement in the new function is used to check if the contract has already been initialized before. However, the function also uses the init macro which is responsible for initializing the contract. Since the init macro can only be called once per contract, there is no need for an additional check using **require!** to verify whether the contract has been initialized before.

Recommendations: It is recommended to remove the unnecessary **require!** statement to ensure a cleaner and more efficient codebase.

Status: Resolved. Unnecessary **require!** statement was removed.

Finding: #14

Issue: Lack of Configurability for Timeouts in Fast Bridge Service

Severity: Quality Assurance

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/5ed18302ae675e849e0f34b955f0646028946406/src/event_processor.rs
https://github.com/aurora-is-near/fast-bridge-service/blob/5ed18302ae675e849e0f34b955f0646028946406/src/near_events_tracker.rs

Impact: The impact of this issue could result in frustration and inconvenience for users, who may have to retry transactions or experience delays in the confirmation process. Additionally, the lack of configurability may make it difficult for the Fast Bridge project to adapt to changing transaction conditions or network congestion, which could lead to reduced adoption and usage of the system.

Description: The Fast Bridge project has a lack of configurability for timeouts related to transactions. In the code snippet provided, there is a hardcoded timeout of 60 seconds, which may not be sufficient for all transactions. This lack of configurability could result in delays or even failures of transactions, especially in cases where longer confirmation times are required.

Recommendations: To address this issue, it is recommended that the Fast Bridge project implement a more configurable approach for timeouts related to transactions.

Status: Resolved. This is configured only for smoke tests.

Finding: #15

Issue: Wrong parameter on **lp_unlock** near call at **unlock_tokens** in Relayer

Severity: Quality Assurance

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/master/src/unlock_tokens.rs#L24-L27

Impact: Bad Code readability

Description: From Relayer, it passes **{ nonce, proof }** as param to **lp_unlock** call. However, actual near implementation has just one param proof.

Recommendations: As proof includes **nonce** and everything looks good at Near side, we should keep consistency and remove nonce from **lp_unlock** call from **Relayer.**

Status: This was resolved by removing **nonce** from **lp_unlock** call from **Relayer**.

Finding: #16

Issue: Limitations and Risks for Users in the Fast Bridge Project

Severity: Quality Assurance

Where: Documentation

Impact: These limitations and risks can impact the user experience and adoption of the Fast Bridge project. Users may be discouraged from using the bridge due to the higher price and limitations on the tokens that can be transferred. Additionally, the need to contact support to unlock stuck tokens can cause inconvenience and delays.

Description: The Fast Bridge project provides a means for transferring tokens between the NEAR Protocol and Ethereum networks, but it comes with various limitations and risks for users and LP-Relayers. Users may encounter issues such as token lock-up if no relayer is available, requiring them to seek support for unlocking their stuck tokens on NEAR. The transaction size is constrained by relayer liquidity, and only whitelisted tokens can be transferred, albeit at a significantly higher price than the original bridge.

On the other hand, LP-Relayers play a critical role in holding locked tokens on the Ethereum side and facilitating their release on the NEAR side. However, they face their own set of risks and limitations. For instance, there is a potential for double unlock if the relayer already transferred tokens on the Ethereum side and temporarily goes offline. Relayers also require additional maintenance, including liquidity management and key protection. Connectivity issues or server uptime problems can further compound their challenges.

Moreover, if the LP-Relayer is hacked or compromised, several adverse scenarios can unfold. Token theft becomes a possibility, with attackers absconding with locked tokens, leaving users unable to redeem them on NEAR.
Token manipulation is another concern, as a compromised relayer could manipulate token releases for their benefit, potentially exceeding authorized amounts or sending them to unauthorized addresses.
In case of a security breach, the LP-Relayer may need to pause operations, resulting in delayed token releases and causing inconvenience to users.
Lastly, a hack or compromise of the LP-Relayer could harm the reputation of the Fast Bridge project, eroding trust, and impeding its overall adoption and usage.

Recommendation: To mitigate these risks, it is recommended that the Fast Bridge project implement a more decentralized approach that reduces reliance on the relayer and provides greater flexibility and scalability for users.

Status: This issue was resolved in the following ways:

- There won't be a direct loss to the users as they would be able to redeem their tokens on the NEAR side once the lock time is expired.
- Relayer doesn't have any admin access on NEAR side.
- Delayed token release is a part of the decentralized approach by design: there could be multiple relayers that satisfy the requirements of the users. If the relayer doesn't process the transfer for some period of time or is down at all, users can claim their tokens back just by having a delay on it. It's expected that relayers attract users based on their uptime and liquidity; relayers earn a reputation within the process.
- There's also a plan to have a separate relayer/keys for each of the tokens, or depending on the size of the portfolio.

Finding: #17

Issue: Out-of-date Rust Crate Detected with Cargo Audit

Severity: Quality Assurance

Where: https://github.com/aurora-is-near/fast-bridge-service/blob/master/Cargo.toml

Impact:

- **Security Vulnerabilities:** Outdated crates can contain known security vulnerabilities that have been fixed in the newer versions. Using these outdated dependencies can expose the project to potential attacks, compromising the application's security and integrity.
- **Missing Features and Bug Fixes:** Outdated crates may lack new features, optimizations, or bug fixes introduced in the newer versions. This can lead to suboptimal performance, unexpected behavior, or application crashes.

Description: A recent cargo audit has detected an out-of-date Rust crate within the project. Cargo audit is a tool that analyzes the Rust project's dependency tree and reports any known security vulnerabilities or outdated dependencies. Using outdated crates can introduce potential risks and negatively affect the performance, stability, and security of the application.

Recommendations: To address this issue, it is recommended to update the out-of-date crate to its latest version, ensuring that any security vulnerabilities, bug fixes, or new features are incorporated into the project.

Status: Resolved. Out-of-date crate was updated to its latest version.

08 - Disclaimer

The smart contracts provided to AuditOne have been analyzed by the best industry practices at the date of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions). The ethical nature of the project is not guaranteed by a technical audit of the smart contract. Any owner-controlled functions should be carried out by the responsible owner. Before participating in the project, all investors/users are recommended to conduct due research.

The focus of our assessment was limited to the code parts associated with the items defined in the scope. We draw attention to the fact that due to inherent limitations in any software development process and product, an inherent risk exists that even major failures or malfunctions can remain undetected. Further uncertainties exist in any software product or application used during the development, which cannot be free from any errors or failures. These preconditions can impact the system's code and/or functions and/or operation. We did not assess the underlying third-party infrastructure, which adds further inherent risks as we rely on correctly executing the included third-party technology stack itself. Report readers should also consider that over the life cycle of any software product, changes to the product itself or the environment in which it is operated can have an impact leading to operational behaviors other than initially determined in the business specification.

Contact

auditone.io

@auditone_team

hello@auditone.io

A trust layer of our multi-stakeholder world.