SMART CONTRACT AUDIT REPORT

for

MetalInvest

Prepared By: Shuxiao Wang

PeckShield

Oct 25, 2021

Document Properties

Client	MetalInvest
Title	Smart Contract Audit Report
Target	MetalInvest Public Audit
Version	1.0
Author	Yiqun Chen
Auditors	Yiqun Chen, Xuxian Jiang
Reviewed by	Shuxiao Wang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	Oct 25, 2021	Yiqun Chen	Final Release
0.1	Oct 20, 2021	Yiqun Chen	First Draft

Contents

1 | Introduction

Given the opportunity to review the design document and related smart contract source code of the MetalInvest project, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About MetalInvest

MetalInvest is the first platform for tokenized precious metals, enabling everyone to access the $856B+ global metal market. MetalInvest will empower the crypto community with the ability to stabilize their portfolios by investing in real commodities. The basic information of the MetalInvest protocol is as follows:

Table 1.1: Basic Information of The MetalInvest Project

Item	Description
Issuer	MetalInvest
Website	https://metalinvest.org/
Type	Stellar Smart Contract
Platform	Stellar
Audit Method	Whitebox
Latest Audit Report	Oct 25, 2021

In the following, we show the address of the contract used in this audit:

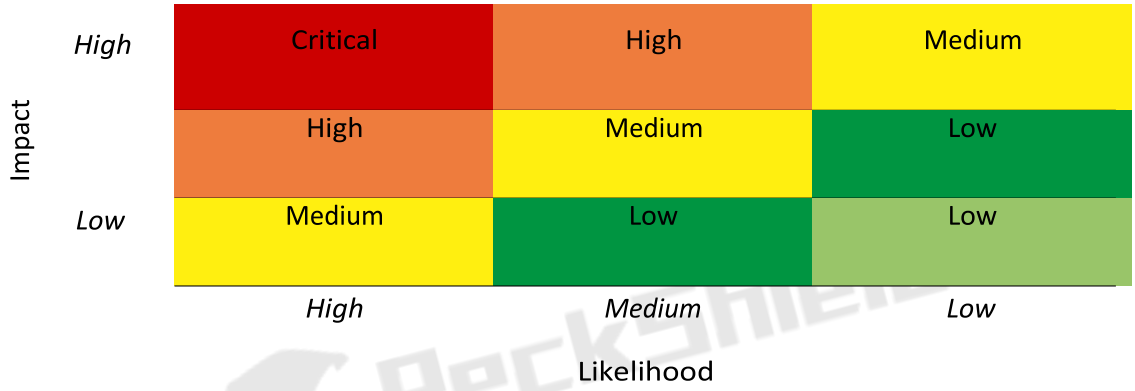
- https://stellar.expert/explorer/public/asset/XAU-GBXJFIGPL7RMHSBLM4HTOOQ37JKSXKMIM6I7FLZVYH4ARQ625Y5YR2Z6
- https://stellar.expert/explorer/public/asset/XAG-GC5W7XYTZNN3MWO7FOVWRUZZQNVKGIGOWNHKIJ3NYCYNA6QW5Y5WMWVK
- https://stellar.expert/explorer/public/asset/XPD-GCWJYGLODM2G43P4BHYAENEU6VNF6AZIM7WRRGUSLW3WXHZH2IQK4MRJ
- https://stellar.expert/explorer/public/asset/XPT-GAFPPZ2KVIJEVQTCWGE5D33RRX7CLBDMOTDQAUUT5S5GVC3K3ZU6NRSZ

- https://stellar.expert/explorer/public/asset/XNI-GAREWGATUELLAK7ZQFOD44JF5U6MPKSXQB4OV64PQE2MYOY7UPK3YYJI
- https://stellar.expert/explorer/public/asset/XLI-GA6D3EMUMRLTQAU2M3PXV77KHKAJ2HFNHCRASHY4UTNNKZD45NAHUQ4H
- https://stellar.expert/explorer/public/asset/XLI-GA6D3EMUMRLTQAU2M3PXV77KHKAJ2HFNHCRASHY4UTNNKZD45NAHUQ4H
- https://stellar.expert/explorer/public/asset/XTI-GCV5YUMFX2UQXBSVBSQY3YG4XHQIBV36OLA2BG26HLBO6CHCCLMGBXNF
- https://stellar.expert/explorer/public/asset/XCU-GDBD2SKU7SHA5UC6MXT5HZRM4FCEL65RFGOAYC5TSDPIJSA7Q362FNFM

1.2 About PeckShield

PeckShield Inc. [7] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing).

Table 1.2: Vulnerability Severity Classification



1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating *Medium*
Methodology [6]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management

	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices
Special requests	Asset Coverage*

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.

- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [5], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.

Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 | Findings

2.1 Summary

Here is a summary of our findings after analyzing the MetalInvest implementation. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	
Low	1	
Informational	0	
Total	2	

verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerability, and 1 low-severity vulnerability.

Table 2.1: Key MetalInvest Vesting Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Two-Step Transfer Of Privileged Account Ownership	Coding Practices	Confirmed
PVE-002	Low	Suggested Use Of Safemath For claim()	Coding Practices	Fixed

Besides recommending specific countermeasures to mitigate these issues, we also emphasize that it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms need

to kick in at the very moment when the contracts are being deployed in mainnet. Please refer to Section 3 for details.

*Asset Coverage – MetalInvest team provided the proof of ownership of futures contracts or/and options, the value of which covers 100% of the MetalInvest's synthetic assets. This is a satisfying result considering that the rate of margin for most synthetic assets is below 50% (e. Tether).

Also worth mentioning is the fact that the liquidity of these assets is high enough and meets our requirements.

3 | Conclusion

In this audit, we have analyzed the design and implementation of the MetalInvest project. The current code base is clearly organized and those identified issues are promptly confirmed and fixed.

Meanwhile, we need to emphasize that Stellar-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.