CAIRO SECURITY CLAN

VESU MULTIPLY

SECURITY ASSESMENT REPORT

SEPTEMBER 2024

Prepared for

VESU

Contents

1 About Cairo Security Clan

Cairo Security Clan is a leading force in the realm of blockchain security, dedicated to fortifying the foundations of the digital age. As pioneers in the field, we specialize in conducting meticulous smart contract security audits, ensuring the integrity and reliability of decentralized applications built on blockchain technology.

At Cairo Security Clan, we boast a multidisciplinary team of seasoned professionals proficient in blockchain security, cryptography, and software engineering. With a firm commitment to excellence, our experts delve into every aspect of the Web3 ecosystem, from foundational layer protocols to application-layer development. Our comprehensive suite of services encompasses smart contract audits, formal verification, and real-time monitoring, offering unparalleled protection against potential vulnerabilities.

Our team comprises industry veterans and scholars with extensive academic backgrounds and practical experience. Armed with advanced methodologies and cutting-edge tools, we scrutinize and analyze complex smart contracts with precision and rigor. Our track record speaks volumes, with a plethora of published research papers and citations, demonstrating our unwavering dedication to advancing the field of blockchain security.

At Cairo Security Clan, we prioritize collaboration and transparency, fostering meaningful partnerships with our clients. We believe in a customer-oriented approach, engaging stakeholders at every stage of the auditing process. By maintaining open lines of communication and soliciting client feedback, we ensure that our solutions are tailored to meet the unique needs and objectives of each project.

Beyond our core services, Cairo Security Clan is committed to driving innovation and shaping the future of blockchain technology. As active contributors to the ecosystem, we participate in the development of emerging technologies such as Starknet, leveraging our expertise to build robust infrastructure and tools. Through strategic guidance and support, we empower our partners to navigate the complexities of the blockchain landscape with confidence and clarity.

In summary, Cairo Security Clan stands at the forefront of blockchain security, blending technical prowess with a client-centric ethos to deliver unparalleled protection and peace of mind in an ever-evolving digital landscape. Join us in safeguarding the future of decentralized finance and digital assets with confidence and conviction.

2 Disclaimer

Disclaimer Limitations of this Audit:

This report is based solely on the materials and documentation provided by you to Cairo Security Clan for the specific purpose of conducting the security review outlined in the Summary of Audit and Scoped Files. The findings presented here may not be exhaustive and may not identify all potential vulnerabilities. Cairo Security Clan provides this review and report on an "as-is" and "as-available" basis. You acknowledge that your use of this report, including any associated services, products, protocols, platforms, content, and materials, occurs entirely at your own risk.

Inherent Risks of Blockchain Technology:

Blockchain technology remains in its developmental stage and is inherently susceptible to unknown risks and vulnerabilities. This review is specifically focused on the smart contract code and does not extend to the compiler layer, programming language elements beyond the reviewed code, or other potential security risks outside the code itself.

Report Purpose and Reliance:

This report should not be construed as an endorsement of any specific project or team, nor does it guarantee the absolute security of the audited smart contracts. No third party should rely on this report for any purpose, including making investment or purchasing decisions.

Liability Disclaimer:

To the fullest extent permitted by law, Cairo Security Clan disclaims all liability associated with this report, its contents, and any related services and products arising from your use. This includes, but is not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Third-Party Products and Services:

Cairo Security Clan does not warrant, endorse, guarantee, or assume responsibility for any products or services advertised by third parties within this report, nor for any open-source or third-party software, code, libraries, materials, or information linked to, referenced by, or accessible through this report, its content, and related services and products. This includes any hyperlinked websites, websites or applications appearing on advertisements, and Cairo Security Clan will not be responsible for monitoring any transactions between you and third-party providers. It is recommended that you exercise due diligence and caution when considering any third-party products or services, just as you would with any purchase or service through any medium.

Disclaimer of Advice:

FOR THE AVOIDANCE OF DOUBT, THIS REPORT, ITS CONTENT, ACCESS, AND/OR USE, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHOULD NOT BE CONSIDERED OR RELIED UPON AS FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER PROFESSIONAL ADVICE.

3 Executive Summary

This document presents the security review performed by Cairo Security Clan on the Vesu protocol.

Vesu, DeFi's latest progression in the on-chain lending space, is a pioneering platform designed to facilitate fully permissionless, over-collateralized lending agreements. With its ambitious design, Vesu looks to combine the best aspects of both worlds: a liquidity monolith with permissionless, multi-asset lending compartments aka lending pools.Learn more from docs.

The audit was performed using

- manual analysis of the codebase,
- automated analysis tools,
- simulation of the smart contract,
- analysis of edge test cases

1 points of attention, where 0 is classified as Critical, 0 is classified as High, 0 is classified as Medium,0 is classified as Low,1 is classified as Informational and 0 is classified as Best Practices. The issues are summarized in Fig. 1.

This document is organized as follows. Section 1 About Cairo Security Clan. Section 2 Disclaimer. Section 3 Executive Summary. Section 4 Summary of Audit. Section 5 Risk Classification. Section 6 Issues by Severity Levels. Section 7 Test Evaluation.

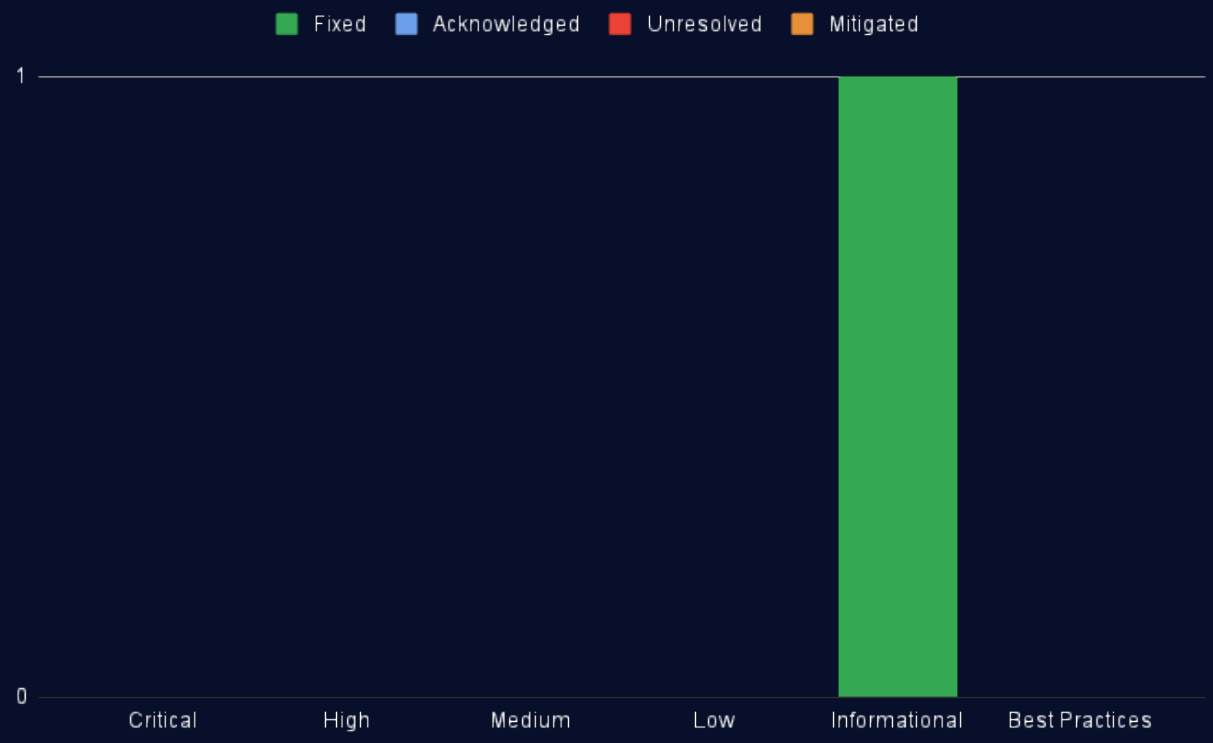

Fig 1: Distribution of issues: Critical (0), **High** (0), **Medium** (0), **Low** (0), **Informational** (1), **Best Practices** (0). **Distribution of status: Fixed** (1), **Acknowledged** (0), **Mitigated** (0), **Unresolved** (0).

4 Summary of Audit

Audit Type	Security Review
Cairo Version	2.6.3
Final Report	31/08/2024
Repository	vesu-multiply
Initial Commit Hash	c4495f14d61977b492aea169dd72d2e18c2d20d6
Final Commit Hash	61cbe861a67173d5c111d0de73561e70c4e91862
Documentation	Website documentation
Test Suite Assessment	High

4.1 Scoped Files

	Contracts
1	/src/multiply.cairo
2	/src/lib.cairo

4.2 Issues

	Findings	Severity	Update
1	Missing sign check for swap amount	Informational	Fixed

5 Risk Classification

The risk rating methodology used by Cairo Security Clan follows the principles established by the CVSS risk rating methodology. The severity of each finding is determined by two factors: **Likelihood** and **Impact**.

Likelihood measures how likely an attacker will uncover and exploit the finding. This factor will be one of the following values:

a) **High**: The issue is trivial to exploit and has no specific conditions that need to be met;

b) **Medium**: The issue is moderately complex and may have some conditions that need to be met;

c) **Low**: The issue is very complex and requires very specific conditions to be met.

When defining the likelihood of a finding, other factors are also considered. These can include but are not limited to Motive, opportunity, exploit accessibility, ease of discovery, and ease of exploit.

Impact is a measure of the damage that may be caused if an attacker exploits the finding. This factor will be one of the following values:

a) **High**: The issue can cause significant damage such as loss of funds or the protocol entering an unrecoverable state;

b) **Medium**: The issue can cause moderate damage such as impacts that only affect a small group of users or only a particular part of the protocol;

c) **Low**: The issue can cause little to no damage such as bugs that are easily recoverable or cause unexpected interactions that cause minor inconveniences.

When defining the impact of a finding other factors are also considered. These can include but are not limited to Data/state integrity, loss of availability, financial loss, and reputation damage. After defining the likelihood and impact of an issue, the severity can be determined according to the table below.

		Likelihood		
		High	**Medium**	**Low**
Impact	**High**	Critical	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Info/Best Practices

To address issues that do not fit a High/Medium/Low severity, Cairo Security Clan also uses three more finding severities: **Informational**, **Best Practices** and **Gas**

a) **Informational** findings do not pose any risk to the application, but they carry some information that the audit team intends to formally pass to the client;

b) **Best Practice** findings are used when some piece of code does not conform with smart contract development best practices;

b) **Gas** findings are used when some piece of code uses more gas than it should be or have some functions that can be removed to save gas.

6 Issues by Severity Levels

6.1 Informational

6.1.1 Missing sign check for swap amount

File(s): /src/multiply.cairo

Description: In the `increase_lever()` function, after a swap operation, the function swap() returns a pair of values: `in_amount` and `out_amount`. Due to the differences between "swap exact in" and "swap exact out" operations, it is necessary to identify which amount corresponds to the collateral and which to the margin using the token address. Then the code assumes that `margin_amount > 0` and `collateral_amount < 0` and proceeds to transfer the amounts and handle the delta accordingly. However, these assumptions are not verified before casting the amounts to `i129_new`.

```
let margin_amount = if margin_swap.route.len() != 0 {
    let (in_amount, out_amount) = self.swap(margin_swap);
    assert!(
        add_margin == 0
            && (out_amount.token == collateral_asset
                || in_amount.token == collateral_asset),
        "invalid-margin_swap-assets"
    );

    let (margin_amount_, collateral_amount_) = if out_amount.token == collateral_asset {
        (in_amount, out_amount)
    } else {
        (out_amount, in_amount)
    };

    // - transfer margin to multiplier
    assert!(
        IERC20Dispatcher { contract_address: margin_amount_.token }
            .transferFrom(
                user, get_contract_address(), margin_amount_.amount.mag.into()
            ),
        "transferFrom-failed"
    );

    // - handleDelta for both (1.)
    handle_delta(
        core,
        margin_amount_.token,
        i129_new(margin_amount_.amount.mag, false),
        get_contract_address()
    );
    handle_delta(
        core,
        collateral_asset,
        i129_new(collateral_amount_.amount.mag, true),
        get_contract_address()
    );
```

A similar issue exists in the `increase_lever()`) and `decrease_lever()` functions when handling leverage swaps.

Recommendation(s): Consider implementing a check to verify the sign of the amounts before casting them to `i129_new`.

Status: Fixed

Update from client: Fixed in commit.

7 Test Evaluation

7.1 Compilation Output

```
scarb build
    Updating git repository github.com/vesuxyz/vesu-v1
   Compiling vesu_multiply v0.1.0 (/.../020-VESU-MULTIPLY/contracts/Scarb.toml)
    Finished release target(s) in 10 seconds
```

7.2 Tests Output

```
scarb test
     Running test vesu_multiply (snforge test)
   Compiling vesu_multiply v0.1.0 (/.../020-VESU-MULTIPLY/contracts/Scarb.toml)
    Finished release target(s) in 11 seconds
Warning:  RPC node with the url starknet-mainnet.public.blastapi.io/rpc/v0_6 uses incompatible version 0.6.0.
     Expected version: 0.7.0


Collected 8 test(s) from vesu_multiply package
Running 0 test(s) from src/
Running 8 test(s) from tests/
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_close (gas: ~9069)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_exact_collateral_withdrawal (gas: ~9235)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_exact_debt_borrow (gas: ~5409)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_margin_asset_swap_exact_out (gas: ~5856)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_margin_asset_swap_exact_in (gas: ~5728)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_withdraw_swap_exact_in (gas: ~9258)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_exact_debt_repay (gas: ~8960)
[PASS] tests::test_multiply::TestMultiply::test_modify_lever_exact_collateral_deposit (gas: ~5417)
Tests: 8 passed, 0 failed, 0 skipped, 0 ignored, 0 filtered out
```