ENIGMA DARK

Securing the Shadows

Security Review

Makina Periphery

Machine Share Oracle

September, 2025

Contents

Summary

Enigma Dark
Enigma Dark is a web3 security firm leveraging the best talent in the space to secure all kinds of blockchain protocols and decentralized apps. Our team comprises experts who have honed their skills at some of the best auditing companies in the industry. With a proven track record as highly skilled white-hats, they bring a wealth of experience and a deep understanding of the technology and the ecosystem.

Learn more about us at enigmadark.com

Makina Periphery: Machine Share Oracle
Makina is a protocol for executing advanced cross-chain investment strategies. It provides the infrastructure for operators to issue tokenized strategies with full DeFi composability and strong risk controls.

The Machine Share Oracle is a smart contract oracle adapter that provides on-chain pricing for shares in both the PreDeposit and Machine cases of the Makina protocol.

Engagement Overview

Over the course of 1.5 days, beginning September 27 2025, the Enigma Dark team conducted a security review of the Makina Periphery: Machine Share Oracle project. The review was performed by two Lead Security Researchers.

The following repositories were reviewed at the specified commits:

Repository	Commit
MakinaHQ/makina-periphery	`45cbca23e3efc9a4f8244c602f685dd3fd1fe8d0`

The scope of the review covered the following files:

```
src
├── factories
|   └── MachineShareOracleFactory
└── oracles
    └── MachineShareOracle
```

Risk Classification

Severity	Description
Critical	Vulnerabilities that lead to a loss of a significant portion of funds of the system.
High	Exploitable, causing loss or manipulation of assets or data.
Medium	Risk of future exploits that may or may not impact the smart contract execution.
Low	Minor code errors that may or may not impact the smart contract execution.
Informational	Non-critical observations or suggestions for improving code quality, readability, or best practices.

Vulnerability Summary

Severity	Count	Fixed	Acknowledged
Critical	0	0	0
High	0	0	0
Medium	0	0	0
Low	0	0	0
Informational	1	0	1

Findings

Index	Issue Title	Status
I-01	Missing address validation in `setMachineShareOracleBeacon`	Acknowledged

Detailed Findings

High Risk

No issues found.

Medium Risk

No issues found.

Low Risk

No issues found.

Informational

I-01 - Missing address validation in `setMachineShareOracleBeacon`

Severity: Informational

Context:

- MachineShareOracleFactory.sol#L67

Technical Details:
The `_machineShareOracleBeacon` address is accepted without validation. This allows the admin to mistakenly set it `address(0)`, which may later cause dependent functions that rely on this beacon to fail or revert:

```
 function setMachineShareOracleBeacon(address _machineShareOracleBeacon)
external restricted {
        MachineShareOracleFactoryStorage storage $ =
_getMachineShareOracleFactoryStorage();
        emit MachineShareOracleBeaconChanged($._machineShareOracleBeacon,
_machineShareOracleBeacon);
        $._machineShareOracleBeacon = _machineShareOracleBeacon;
    }
```

Recommendation:
Add validation to not allow `_machineShareOracleBeacon` to be set as `address(0)` :

```
 function setMachineShareOracleBeacon(address _machineShareOracleBeacon)
external restricted {
+     require (_machineShareOracleBeacon != address(0), "invalid address");
        MachineShareOracleFactoryStorage storage $ =
_getMachineShareOracleFactoryStorage();
        emit MachineShareOracleBeaconChanged($._machineShareOracleBeacon,
_machineShareOracleBeacon);
        $._machineShareOracleBeacon = _machineShareOracleBeacon;
    }
```

Developer Response:
Acknowledged.

Annex

Annex A: PreDepositVault Share Price Behavior and Fuzz Test Analysis

Context:

- While writing fuzz tests for the `MachineShareOracle`, the Makina team observed the following behavior in getSharePrice.t.sol#L72-L109 for a fixed amount of machine shares (`shares1`): the output of `previewRedeem(shares1)` varies depending on the price of the `depositToken` relative to its underlying `accountingToken`.
    - When the `depositToken` price increases, `previewRedeem` returns fewer assets than expected.
    - When the `depositToken` price decreases, `previewRedeem` returns more assets.
- This implies that under negative-yield scenarios, users could redeem more `depositToken` than initially deposited, potentially leaving subsequent redeemers unable to recover their full share balances.

Technical Details:
The behavior originates from the PDV's share price calculation, which includes a virtual asset adjustment via the + dtUnit term in the numerator:

```
assets = shares * (dtBal + dtUnit / price_d_a) / (stSupply + 10 ** offset)
```

where:

- `dtBal`: deposit token balance
- `price_d_a`: depositToken/accountingToken price ratio
- `virtualAssets = dtUnit / price_d_a`
- `virtualShares = 10 ** offset`

Unlike the fixed virtual constants used in standard ERC-4626 vaults, `virtualAssets` here depends inversely on price (1 / `price_d_a`). As the deposit token depreciates, the virtual asset term grows, causing overestimation of `previewRedeem` results.

This mirrors known behavior in ERC-4626 vaults with non-trivial virtual assets, such as Euler's implementation (which uses `1e6` instead of OpenZeppelin's `1 wei`), where the effect becomes noticeable in low-liquidity or high-volatility scenarios.

Developer Resolution:
The Makina team confirmed the underlying mechanism and chose to retain the current formulation for now, with plans to revisit it in future iterations of the PDV (PreDepositVault). A potential mitigation under consideration involves simplifying the PDV into a 1:1 wrapper over the `depositToken` (analogous to WETH wrapping ETH), with adjustments for decimal mismatches when the deposit token does not use 18 decimals.

Disclaimer

This report does not endorse or critique any specific project or team. It does not assess the economic value or viability of any product or asset developed by parties engaging Enigma Dark for security assessments. We do not provide warranties regarding the bug-free nature of analyzed technology or make judgments on its business model, proprietors, or legal compliance.

This report is not intended for investment decisions or project participation guidance. Enigma Dark aims to improve code quality and mitigate risks associated with blockchain technology and cryptographic tokens through rigorous assessments.

Blockchain technology and cryptographic assets inherently involve significant risks. Each entity is responsible for conducting their own due diligence and maintaining security measures. Our assessments aim to reduce vulnerabilities but do not guarantee the security or functionality of the technologies analyzed.

This security engagement does not guarantee against a hack. It is a review of the codebase during a specific period of time. Enigma Dark makes no warranties regarding the security of the code and does not warrant that the code is free from defects. By deploying or using the code, the project and users of the contracts agree to use the code at their own risk. Any modifications to the code will require a new security review.