OpenVM
Security Review

Cantina Managed review by:

Guido Vranken, Lead Security Researcher
Kcharbon, Security Researcher

May 3, 2025

Contents

1 Introduction

1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

1.2 Disclaimer

Cantina Managed provides a detailed evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While Cantina Managed endeavors to identify and disclose all potential security issues, it cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities that were absent during the initial review. Therefore, any changes made to the code require a new security review to ensure that the code remains secure. Please be advised that the Cantina Managed security review is not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

1.3 Risk assessment

Severity	Description
Critical	*Must* fix as soon as possible (if already deployed).
High	Leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.
Medium	Global losses <10% or losses to only a subset of users, but still unacceptable.
Low	Losses will be annoying but bearable. Applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.
Gas Optimization	Suggestions around gas saving practices.
Informational	Suggestions around best practices or readability.

1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. Critical findings have a high likelihood of being exploited and must be addressed immediately. High findings are almost certain to occur, easy to perform, or not easy but highly incentivized thus must be fixed as soon as possible.

Medium findings are conditionally possible or incentivized but are still relatively likely to occur and should be addressed. Low findings a rare combination of circumstances to exploit, or offer little to no incentive to exploit but are recommended to be addressed.

Lastly, some findings might represent objective improvements that should be addressed but do not impact the project's overall security (Gas and Informational findings).

2 Security Review Summary

OpenVM is a performant and modular zkVM framework built for customization and extensibility.

From Apr 22nd to Apr 24th the Cantina team conducted a review of openvm on commit hash 0f94c8a3. The team identified a total of **1** issues:

Issues Found

Severity	Count	Fixed	Acknowledged
Critical Risk	0	0	0
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	0	0	0
Gas Optimizations	0	0	0
Informational	1	0	0
Total	**1**	**0**	**0**

3 Findings

3.1 Informational

3.1.1 Manipulation of `proofData.offset` can lead to unpredictable behavior

Severity: Informational

Context: *(No context files were provided by the reviewer)*

Description: In the `OpenVmHalo2Verifier` contract template, the `_constructProof` function relies on the `proofData.offset` value in inline assembly to properly copy over the KZG accumulator and proof suffix values into the calldata that is sent to the `Halo2Verifier` contract. This offset value can be manipulated by the caller to be larger than expected from abi encoding standards.

This could lead to unintended behavior as the values copied over into the final proof wouldn't be accurate. This is only informational since this security check needs to happen on the client side when they construct their smart contract that would then call this verifier contract. It also wouldn't apply to anyone writing their contracts in solidity.

Recommendation: Perhaps a warning in the documentation that this contract assumes proper abi-encoded inputs. Not needed though as almost all contracts assume this.