< Back to articles

Zunami: UZD Audit Summary

Andrea Nováková // AUDITS, ETHEREUM SEPTEMBER 26, 2022

Update (18th August 2023): this audit report was performed on commit 53dc20a. The hack was performed by a donation (price manipulation) into strategy MimCurveStakeDAO (step 3) that was first added in commit `6df0ae533a718a34df70984d745cc2d70fb7172d` and was not in the scope of this audit.

Zunami engaged Ackee Blockchain to review and audit the Zunami UZD between **September 12 and 16, 2022**. The entire audit process was conducted with a total time commitment of **4**

engineering days. We now publish a summary of our results.

METHODOLOGY

We start by reviewing the specifications, sources, and instructions provided to us, which is essential to ensure we understand the project's size, scope, and functionality. This is followed by due diligence using the static analysis tools Wake and Slither.

In addition to tool-based analysis, we continue with a detailed manual code review, which is the process of reading the source code line by line to identify potential vulnerabilities or code duplications. When the code review is complete, we run unit tests to ensure the system works as expected and potentially write missing unit or fuzzy tests. We also deploy the contracts locally and try to attack and break the system.

SCOPE

We audited commit *53dc20a* of the ZunamiProtocol/ZunamiStable repository.

During the security review, **we paid particular attention to**:

- ensuring the price caching can not be exploited;
- deposit/withdrawal limits can not cause DoS;
- detecting possible reentrancies in the code;
- ensuring access controls are not too relaxed or too strict;
- looking for common issues such as data validation.

FINDINGS

Here we present our findings.

Critical severity

No critical severity issues were found.

High severity

H1: Anybody can cause DoS of the protocol if the limits are set

H2: Daily deposit/withdrawal limits can be violated

H3: The previewWithdraw function does not include fee calculation

Medium severity

M1: Fees can be set to 100% anytime

M2: Two-phase transfer of ownership

M3: Renounce ownership

Low severity

No low severity issues were found.

Warning severity

W1: Support for the meta-transactions

W2: Variable shadowing of the owner variable

W3: Floating pragma

W4: Usage of solc optimizer

W5: Missing package-lock.json

Informational severity

I1: Unnecessary call for currentAssetPrice

I2: Functions that could be external

I3: Typos

CONCLUSION

Our review resulted in **14 findings** ranging from *Informational* to *High* severity.

The most severe one was the possibility of DoS (H1).

We recommended Zunami to:

- fix all high severity issues since it is not recommended for deployment and use in this state;

- reconsider Trust model of the protocol as long as it heavily depends on Owner;
- create documentation, including NatSpec code comments;
- address all other reported issues.

Update: Zunami provided an updated codebase that addresses the reported issues. We reviewed commit 335b852 on **September 23, 2022**. The scope was only related to the issues identified in this report.

All findings were acknowledged and some of them (H2, H3, M1, M2, W2, W5, I1, I3) were fixed. **The safety of the protocol now depends on the protocol administrators** and the parameters they set up (such as withdraw/deposit limits), see the discussion of issue H1 in the full audit report.

Ackee Blockchain's full *Zunami UZD* audit report with a more detailed description of all findings and recommendations can be found here.

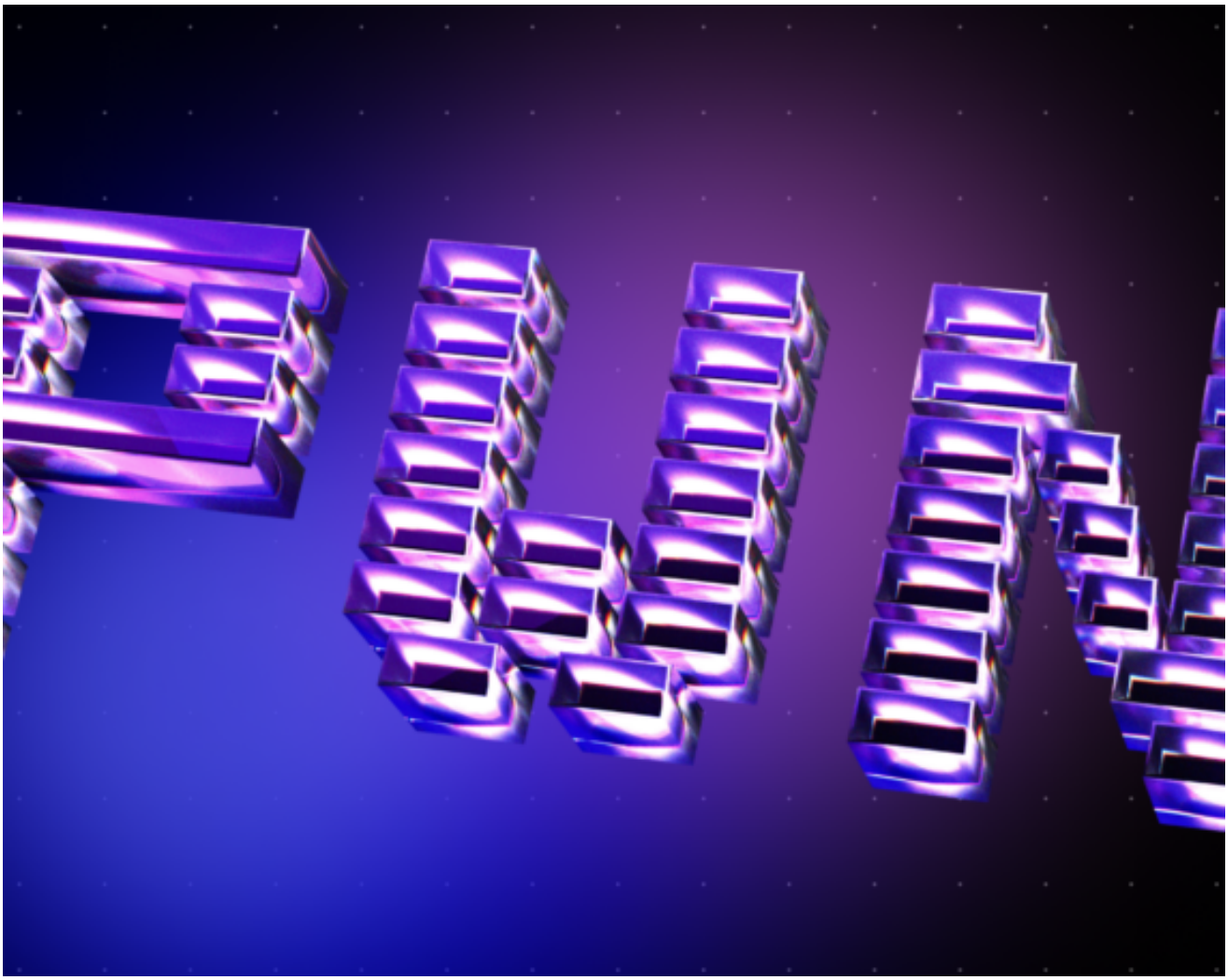
Audit Blockchain Ethereum EVM Security Smart Contract Solidity Woke Zunami.Protocol

Andrea Nováková

You May Also Like

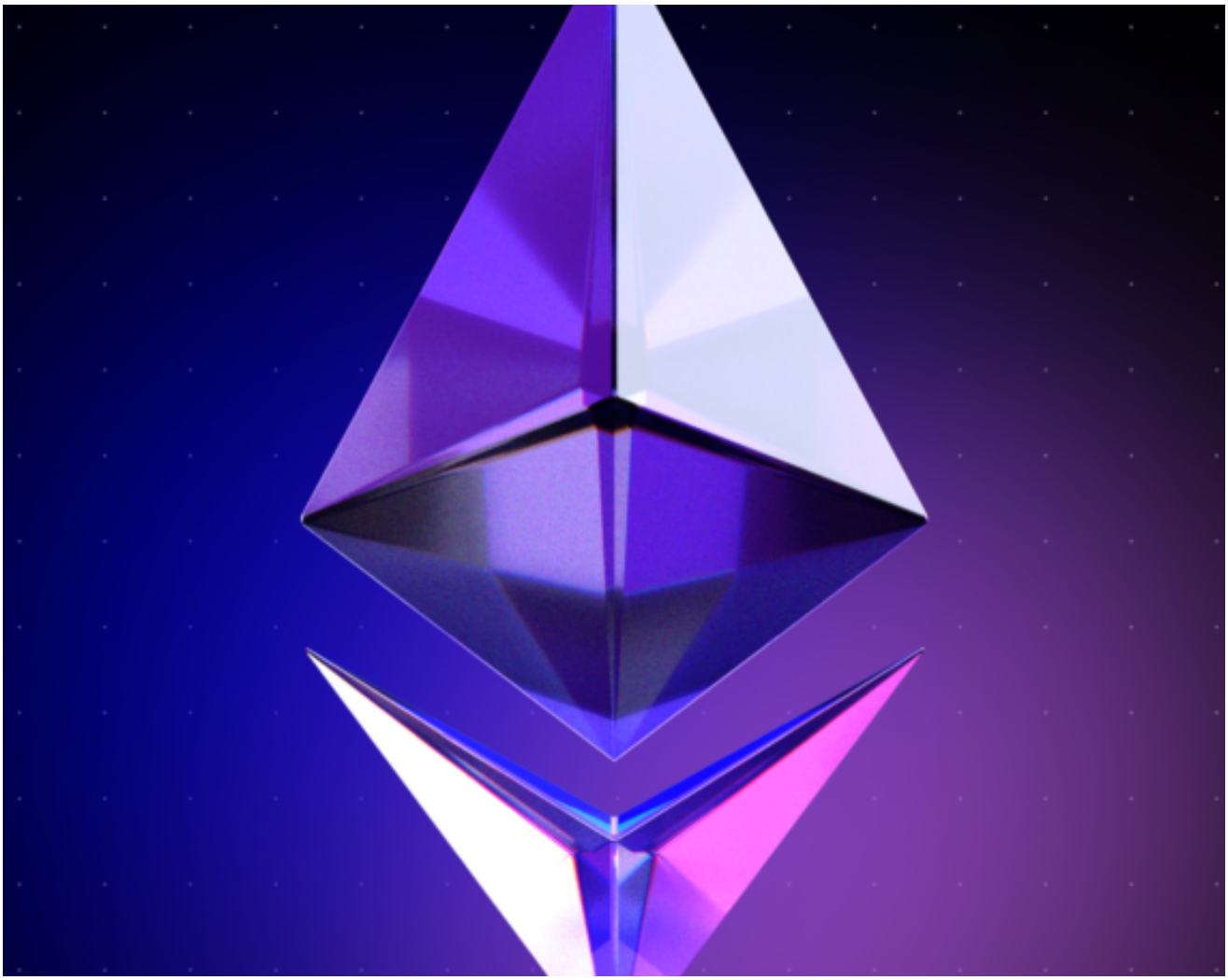
// AUDITS, ETHEREUM, WAKE FEBRUARY 12, 2025

Leech Protocol Audit Summary



// AUDITS ETHEREUM WAKE FEBRUARY 6, 2025

PWN Protocol Audit Summary



// EDUCATION NOVEMBER 27, 2024

Ethereum’s Pectra upgrade from the security perspective