Immunefi
immunefi.com

Puffer Finance Boost Summary Report

Content Index

Overview

Immunefi Boosts are special, time-limited events that supercharge the reach and visibility of programs to our whitehat community.

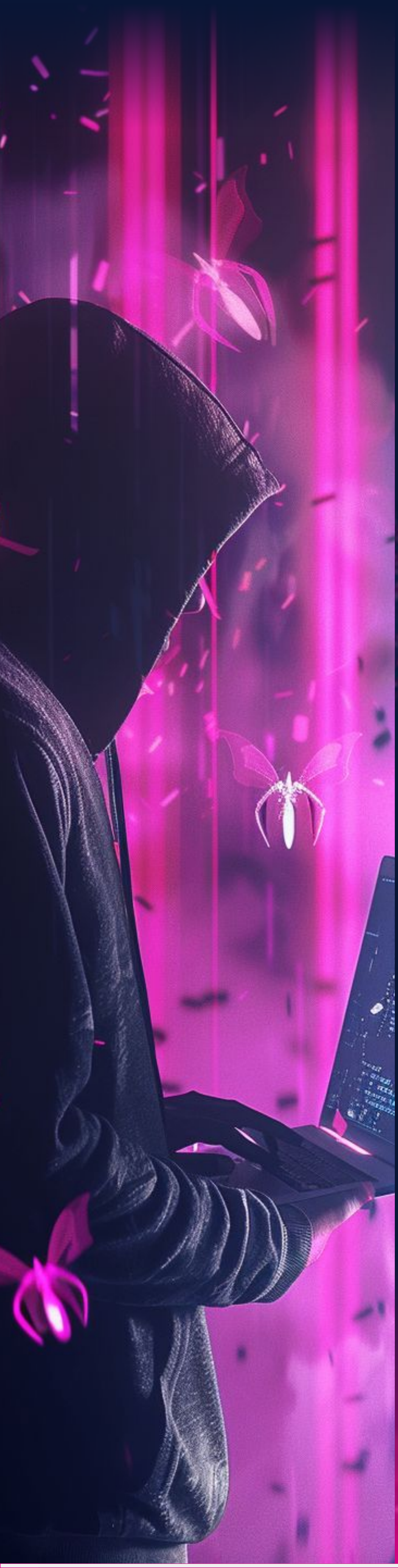
From February 22 to March 7, 2024, the Puffer Finance Boost offered $50,000 USD in guaranteed rewards, in addition to per-unique bug rewards depending on the severity of the finding: Critical ($200k), High ($50k), Medium ($2k), and Low ($1k), giving researchers an extra incentive to hunt.

Immunefi's Discord server hosted a channel for enhanced, two-way communication between whitehats and the Puffer Finance team, improving feedback and response times. Managed Triaging was also activated for the duration of this event, streamlining the resolution process for incoming bug reports.

During this event, 9 low bugs, 5 medium bugs, and 23 insight reports were found on the target contracts. A total of 49 security researchers participated.

Puffer Finance distributed the $50k baseline reward pool to 36 of the very best submissions for the security researchers' valiant efforts, including "Insight" submissions scored on a rating system that takes into account levels of:

- 1) Security best practices
- 2) Code optimizations and enhancements
- 3) Architectural decentralization and composability
- 4) Documentation improvements



Puffer Finance Introduction

Puffer is a decentralized native liquid restaking protocol (nLRP) built on Eigenlayer. It makes native restaking on Eigenlayer more accessible, allowing anyone to run an Ethereum Proof of Stake (PoS) validator while supercharging their rewards.

The current scope is only to examine the set of smart contracts already deployed. These smart contracts allow the depositing of stETH and allow a multisig to sign off on a transaction to deposit the stETH assets to the EigenLayer stETH Strategy smart contract.

For more information about Puffer Finance, please visit https://www.puffer.fi/

Scope Of Assets

The target assets in scope for the Boost were Puffer Finance smart contracts. Puffer Depositor swap functions were in scope, but due to them being paused, bugs were only be considered if they could bypass the pause mechanism.

The Puffer Finance codebase for the Boost was available at: https://github.com/PufferFinance/pufETH/tree/main

The total nSLOC was 792.

Summary

Duration:
Two weeks

Boost date:
22 Feb 2024 - 07 Mar 2024

Rewards pool:
$50k baseline rewards

nSLOC:
792

Submitted reports:
109

Security researchers:
49

Valid vulnerabilities:
14

Insight reports:
23

Total Whitehat Participation By Tier

Total	49

Leaderboard

Position	Reward	Username	Valids	Insights
1	$9,276	codesentry	2	0
2	$6,692	OxSCSamurai	1	3
3	$6,390	OxDEADBEEF	3	0
4	$5,143	LokiThe5th	2	1
5	$3,249	shadowHunter	1	0
6	$2,499	cheatcode	1	2
7	$1,699	aman	1	0
8	$1,699	dontonka	1	0
9	$1,699	yixxas	1	0
10	$1,699	MahdiKarimi	1	0
11	$1,699	grobelr	1	0
12	$1,595	MrPotatoMagic	1	3

Position	Reward	Username	Valids	Insights
13	$1,200	SAAJ	0	3
14	$1,195	Kodak	1	2
15	$955	kaysoft	1	1
16	$955	Kenzo	1	1
17	$800	djxploit	0	2
18	$715	Norah	1	0
19	$715	HX000	1	0
20	$715	honeymewn	1	0
21	$560	offside0011	0	2
22	$400	oxumarkhatab	0	2
23	$400	jaraxxus	0	1
24	$400	chainSiren	0	1

Total Whitehat Participation By Tier

Total	49

Leaderboard

Position	Reward	Username	Valids	Insights
25	$400	ox7a69	0	1
26	$400	Shaheen	0	1
27	$320	ihtishamsudo	0	2
28	$240	OxJoyBoy03	0	1
29	$240	SentientX	0	1
30	$240	Cryptor	0	1
31	$240	ladboy233	0	1
32	$240	Haxatron	0	1
33	$160	marqymarq10	0	1
34	$80	crazy_squirrel	0	1
35	$80	imaybeghost	0	1

Top 5 Best Reports

User will lose funds

Report number: 28613

Submitted by: @shadowHunter

Target: https://etherscan.io/address/0xd9a442856c234a39a81a089c06451ebaa4306a72

Impacts:

- Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield

Program Action: Confirmed as medium severity.

Bug Description:

In case of slashing, Lido `claimWithdrawal` will give discounted value which is lesser than expected ETH.

This causes huge problem since `$.lidoLockedETH` does not account for discount, causing `totalAssets` to become higher than required.

This indirectly causes share prices to become higher since share price increases with increased `totalAssets`.

Timelock transaction that consume more then 209_595 gas will not be executed but the upper transaction will succeed

Report number: 28623

Submitted by: @OxDEADBEEF

Target:
https://etherscan.io/address/0xd9a442856c234a39a81a089c06451ebaa4306a72

Impacts:

- Temporary freezing of funds for at least 1 hour
- Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol)
- Contract fails to deliver promised returns, but doesn't lose value

Program Action: Confirmed as low severity.

Bug Description:

The timelock's `executeTransaction` does not validate that it has enough gas to execute the underlying transaction.

Because of eip-150's `63/64` gas rule - transactions that need more then `209_595` gas to execute can fail due to out of gas while the parent transaction transaction has enough gas (1/64) to successfully finish the transaction

Deposit of stETH fails due to LIDO's 1-2 wei cornor issue

Report number: 28663

Submitted by: @codesentry

Target: https://etherscan.io/address/0x7276925e42f9c4054afa2fad80fa79520c453d6a

Impacts:
- Contract fails to deliver promised returns, but doesn't lose value

Program Action: Confirmed as low severity..

Bug Description:

`depositStETH` method of `PufferDepositor` contract transfer stETH from `msg.sender` to `PufferDepositor` and then `PufferVault` transfer it from `PufferDepositor`. Overall `depositStETH` may fails randomly because of random 1 wei cornor issue in LIDO's stETH.

stETH balance calculation includes integer division, and there is a common case when the whole stETH balance can't be transferred from the account while leaving the last 1-2 wei on the sender's account. The same thing can actually happen at any transfer or deposit transaction.

This issue is documented here(lidofinance/lido-dao#442) and still an valid issue.

Same is documented in LIDO's official document (https://docs.lido.fi/guides/lido-tokens-integration-guide/) also.

pufETH/src/Timelock.sol::executeTransaction() - This bug makes it possible to unexpectedly execute a timelocked queued transaction TWICE, accidentally/mistakenly.

Report number: 28777

Submitted by: @OxSCSamurai

Target: https://etherscan.io/address/0x3C28B7c7Ba1A1f55c9Ce66b263B33B204f2126eA#code

Impacts:

- Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol)
- Protocol at risk of getting queued transactions executed more than once

Program Action: Confirmed as low severity.

Bug Description:

- This bug makes it possible to unexpectedly execute a timelocked queued transaction more than once, ACCIDENTALLY/MISTAKENLY.
- This vulnerability/risk does NOT require attacker access to privileged addresses/multisigs, because there is no attacker to begin with.
- Due to this bug, ACCIDENTAL actions can lead to unfavorable/unacceptable impacts/risks on the protocol or users.

Insecure Token Allowance Management in PufferDepositor Contract

Report number: 29110

Submitted by: @cheatcode

Target:
https://etherscan.io/address/0x7276925e42f9c4054afa2fad80fa79520c453d6a

Impacts:

- Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield

Program Action: Acknowledged and closed. Rewarded as insight report.

Bug Description:

The `PufferDepositor` contract fails to properly manage token allowances for swap service routers (like 1Inch or SushiSwap) after executing token swap operations. This can lead to potential security risks and unnecessary resource wastage on the blockchain.