Audit Competition

Summary Report
April 2025

Content Index

Overview

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

From March 11, 2025 to March 25, 2025, the Yeet Competition offered up to $30,000 USD in rewards for security researchers.

Immunefi's Discord server hosted a channel for enhanced, two-way communication between whitehats and the Yeet 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, 33 critical bugs, 21 high, 11 medium bugs, 14 low, and 40 insight reports were found on the target contracts. A total of 263 security researchers participated.

Yeet distributed the $30k reward pool to 72 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

Yeet Introduction

Yeet is a gamified DeFi protocol on Berachain that offers an interactive financial experience through strategy and timing. Its core feature, the Yeet Game, allows users to deposit BERA tokens into a pool, with the last depositor winning most of the funds. YeetBonds help protocols manage their liquidity efficiently, while Yeetard NFTs provide additional in-game benefits.

The native $YEET token can be farmed and staked for rewards. By integrating game mechanics into DeFi, Yeet fosters community engagement, liquidity solutions, and a unique way to participate in decentralized finance.

For more information about Yeet, please visit https://www.yeetit.xyz/

Yeet provides rewards in USDC, denominated in USD.

Scope Of Assets

The target assets in scope for the Audit Competition were Yeet's smart contracts.

The total nSLOC was 1,538.

Summary

Duration: **Two weeks**	Comp Date: **11 Mar 2025 - 25 Mar 2025**	Rewards Pool: **$30,000**	nSLOC: **1,538**
Submitted reports: **943**	Security researchers: **263**	Valid vulnerabilities: **79**	Insight reports: **40**

Total Whitehat Participation

263
Total Researchers

72
Paid Researchers

Leaderboard

Position	Reward	Username	Valids	Insights
1	$7,691	merlinboii	5	1
2	$4,222	kmm	3	0
3	$4,099	max10afternoon	1	0
4	$4,002	trtrth	4	3
5	$3,384	RNemes	1	0
6	$1,150	robin_bl4z3	1	1
7	$484	yesofcourse	1	0
8	$425	Oxl33	4	1
9	$274	NHristov	1	0
10	$233	DoD4uFN	2	2
11	$218	OxAnmol	2	0
12	$218	cryptostaker	2	0
13	$218	kaysoft	2	0
14	$184	coffiasd	2	0
15	$154	Ragnarok	2	2
16	$146	Minnow80539	1	0
17	$146	OldDingo56530	1	0
18	$132	dobrevaleri	2	1
19	$110	Oxgritty	2	0
20	$110	nnez	2	0
21	$109	BenR	1	1
22	$94	Bluedragon	1	1
23	$87	Yaneca_b	2	0
24	$87	pontifex	2	0
25	$82	peppef	1	2
26	$75	x60scs	1	1

Position	Reward	Username	Valids	Insights
27	72	X0sauce	1	0
28	72	p0wd3r	1	0
29	72	Ace30	1	0
30	72	valy001	1	0
31	72	Le_Rems	1	0
32	59	chista0x	0	2
33	59	h2134	0	4
34	56	Oxrochimaru	1	1
35	49	DSbeX	1	0
36	49	zaevlad	1	0
37	49	MarsKittyHacker	1	0
38	49	T0_Socrates	1	0
39	44	pxng0in	0	2
40	44	Victor_TheOracle	0	2
41	38	rajkaur	1	0
42	38	armormadeofwoe	1	0
43	38	Pyro	1	0
44	38	InquisitorScythe	1	0
45	38	zeroK	1	0
46	38	aksoy	1	0
47	38	whitehatanon1	1	0
48	38	aman	1	0
49	38	vladi319	1	0
50	38	Oxodus	1	0
51	38	Ekko	1	0
52	38	testnate	1	0
53	38	hustling0x	1	0
54	38	greed	1	0
55	38	Oxgee001	1	0
56	38	Invcbull	1	0
57	38	Bani70	1	0
58	38	KaptenCrtz	1	0
59	38	x0bserver	1	0
60	38	libro9595	1	0
61	37	Oxbakeng	0	1

Position	Reward	Username	Valids	Insights
62	37	ZeroXGondar	0	1
63	37	OxSimao	0	1
64	30	perseverance	0	2
65	22	styphoiz	0	1
66	22	k1k1	0	1
67	22	p3nc1l	0	1
68	22	Nawsanders	0	1
69	22	Oxblackadam	0	1
70	22	Dimaranti	0	1
71	7	xdead4f	0	1
72	7	Exp10its	0	1

Top 3 Reports

StakeV2: Inconsistencies in totalSupply computation, can lead to protocol insolvency

Report number: 41215

Submitted by: @max10afternoon

Target:
https://github.com/immunefi-team/audit-comp-yeet/blob/main/src/StakeV2.sol

Impacts:

- Protocol insolvency

Program Action: Confirmed as critical severity.

Report Excerpt:

Unstaking will decrease the totalSupply, by the amount being unstaken, but won't transfer the tokens until, the unstake process gets completed. This will effect the computation of accumulatedDeptRewardsYeet. Meaning that the unstaken amount will be distributable as reward, making the protocol insolvent.

Attacker can DoS `StakeV2`'s rewards distribution by repeatedly inflating Zapper's approval for whitelisted Kodiak Vault tokens

Report number: 41432

Submitted by: @merlinboii

Target:
https://github.com/immunefi-team/audit-comp-yeet/blob/main/src/contracts/Zapper.sol

Impacts:

- Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol)
- Permanent freezing of unclaimed yield

Program Action: Confirmed as high severity.

Report Excerpt:

An attacker can **repeatedly inflate the Zapper's approval** for any **whitelisted Kodiak Vault tokens** that are **targeted for distribution as StakeV2 rewards.** This leads to a **Denial-of-Service (DoS) on rewards distribution** due to an **overflow revert in safeIncreaseAllowance()**, without incurring any direct cost other than gas fees.

Permanent freezing of yield due to incorrect reward handling in `StakeV2` claim functions

Report number: 41280

Submitted by: @merlinboii

Target:
https://github.com/immunefi-team/audit-comp-yeet/blob/main/src/StakeV2.sol

Impacts:

- Contract fails to deliver promised returns, but doesn't lose value
- Permanent freezing of unclaimed yield

Program Action: Confirmed as high severity.

Report Excerpt:

Users claiming rewards through `StakeV2`'s claim functions: `claimRewardsInNative()`, `claimRewardsInToken0()`, `claimRewardsInToken1()` and `claimRewardsInToken()`, which are designed to handle reward claims in a single output token (either native, token0, token1, or a whitelisted token) can **permanently lose access to a portion of their rewards**.

This occurs because the `Zapper` contract incorrectly sends any remaining token debt to `StakeV2` instead of the user who initiated the claim. Since `StakeV2` has no mechanism to recover or redistribute these tokens, the lost funds become permanently inaccessible to the user.

End of Report