



# VRust

## **Security Assessment**

O2Lab VRust Team

11/04/2022 19:29:02

## Contents

<b>Summary</b>	<b>5</b>
<b>Overview</b>	<b>6</b>
Project Summary . . . . .	6
Audit Summary . . . . .	6
Vulnerability Summary . . . . .	6
<b>Findings</b>	<b>7</b>
<b>Finding Statistic</b>	<b>8</b>
<b>Issue: 0: IntegerFlow</b>	<b>10</b>
<b>Issue: 1: IntegerFlow</b>	<b>12</b>
<b>Issue: 2: IntegerFlow</b>	<b>14</b>
<b>Issue: 3: IntegerFlow</b>	<b>16</b>
<b>Issue: 4: IntegerFlow</b>	<b>18</b>
<b>Issue: 5: IntegerFlow</b>	<b>20</b>
<b>Issue: 6: IntegerFlow</b>	<b>22</b>
<b>Issue: 7: IntegerFlow</b>	<b>24</b>
<b>Issue: 8: IntegerFlow</b>	<b>26</b>
<b>Issue: 9: IntegerFlow</b>	<b>28</b>
<b>Issue: 10: MissingKeyCheck</b>	<b>30</b>
<b>Issue: 11: MissingKeyCheck</b>	<b>32</b>
<b>Issue: 12: MissingKeyCheck</b>	<b>34</b>
<b>Issue: 13: MissingKeyCheck</b>	<b>36</b>
<b>Issue: 14: MissingKeyCheck</b>	<b>38</b>
<b>Issue: 15: MissingKeyCheck</b>	<b>40</b>

<b>Issue: 16: MissingKeyCheck</b>	<b>42</b>
<b>Issue: 17: MissingKeyCheck</b>	<b>44</b>
<b>Issue: 18: MissingKeyCheck</b>	<b>46</b>
<b>Issue: 19: MissingKeyCheck</b>	<b>48</b>
<b>Issue: 20: MissingKeyCheck</b>	<b>50</b>
<b>Issue: 21: MissingKeyCheck</b>	<b>52</b>
<b>Issue: 22: MissingKeyCheck</b>	<b>54</b>
<b>Issue: 23: TypeConfusion</b>	<b>56</b>
<b>Issue: 24: TypeConfusion</b>	<b>62</b>
<b>Issue: 25: TypeConfusion</b>	<b>64</b>
<b>Issue: 26: TypeConfusion</b>	<b>66</b>
<b>Issue: 27: TypeConfusion</b>	<b>68</b>
<b>Issue: 28: TypeConfusion</b>	<b>70</b>
<b>Issue: 29: TypeConfusion</b>	<b>76</b>
<b>Issue: 30: TypeConfusion</b>	<b>82</b>
<b>Issue: 31: TypeConfusion</b>	<b>83</b>
<b>Issue: 32: TypeConfusion</b>	<b>87</b>
<b>Issue: 33: TypeConfusion</b>	<b>88</b>
<b>Issue: 34: TypeConfusion</b>	<b>92</b>
<b>Issue: 35: TypeConfusion</b>	<b>96</b>
<b>Issue: 36: TypeConfusion</b>	<b>99</b>
<b>Appendix</b>	<b>101</b>
Finding Categories . . . . .	101
Gas Optimization . . . . .	101

Mathematical Operations . . . . .	101
Logical Issue . . . . .	101
Language Specific . . . . .	101
Coding Style . . . . .	101
Checksum Calculation Method . . . . .	101
<b>Disclaimer</b>	<b>103</b>

## Summary

This report has been prepared for O2Lab VRust Team to discover issues and vulnerabilities in the source code of the O2Lab VRust Team project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques. The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

## Overview

### Project Summary

Project Name	O2Lab VRust Team
Platform	Ethereum
Language	Solana
Crate	mpl_metaplex
GitHub Location	<a href="https://github.com/parasol-aser/vrust">https://github.com/parasol-aser/vrust</a>
sha256	Unknown

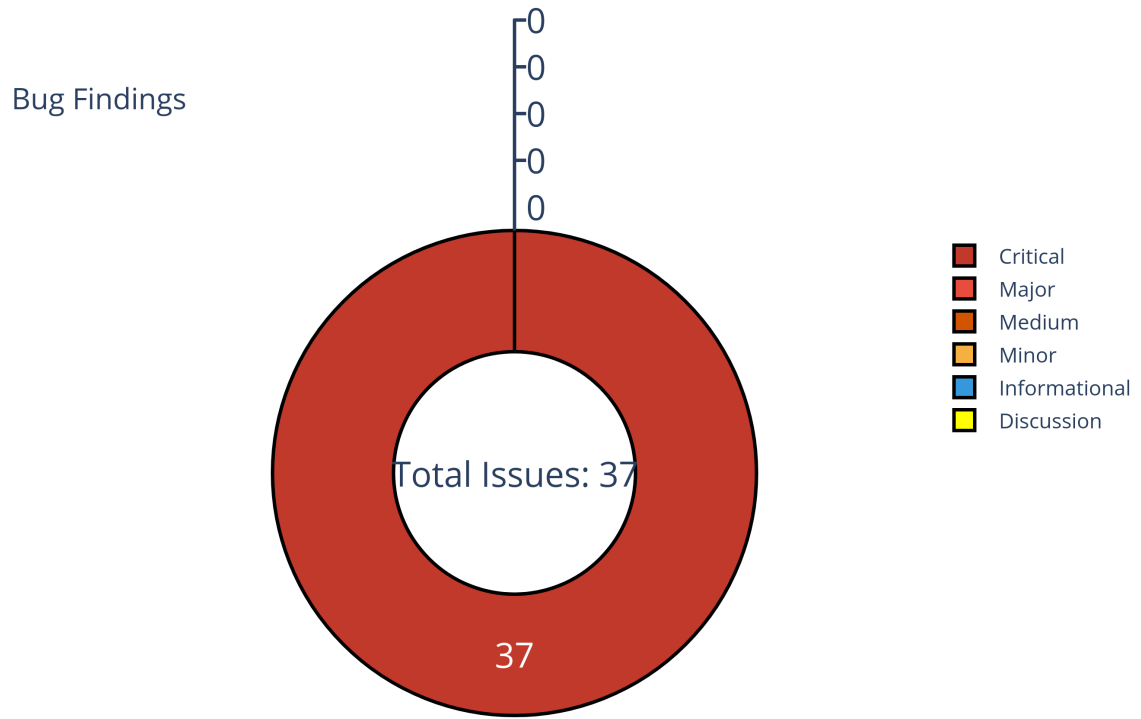
### Audit Summary

Delivery Date	11/04/2022
Audit Methodology	Static Analysis
Key Components	

### Vulnerability Summary

Vulnerability Level	Total
Critical	37
Major	0
Medium	0
Minor	0
Informational	0
Discussion	0

## Findings



**Figure 1:** Findings

## Finding Statistic

Category	Count
IntegerFlow	10
MissingKeyCheck	13
TypeConfusion	14

ID	Category	Severity	Status
0	IntegerFlow	Critical	UnResolved
1	IntegerFlow	Critical	UnResolved
2	IntegerFlow	Critical	UnResolved
3	IntegerFlow	Critical	UnResolved
4	IntegerFlow	Critical	UnResolved
5	IntegerFlow	Critical	UnResolved
6	IntegerFlow	Critical	UnResolved
7	IntegerFlow	Critical	UnResolved
8	IntegerFlow	Critical	UnResolved
9	IntegerFlow	Critical	UnResolved
10	MissingKeyCheck	Critical	UnResolved
11	MissingKeyCheck	Critical	UnResolved
12	MissingKeyCheck	Critical	UnResolved
13	MissingKeyCheck	Critical	UnResolved
14	MissingKeyCheck	Critical	UnResolved
15	MissingKeyCheck	Critical	UnResolved
16	MissingKeyCheck	Critical	UnResolved
17	MissingKeyCheck	Critical	UnResolved
18	MissingKeyCheck	Critical	UnResolved
19	MissingKeyCheck	Critical	UnResolved



ID	Category	Severity	Status
20	MissingKeyCheck	Critical	UnResolved
21	MissingKeyCheck	Critical	UnResolved
22	MissingKeyCheck	Critical	UnResolved
23	TypeConfusion	Critical	GitHub Link to be added.
24	TypeConfusion	Critical	GitHub Link to be added.
25	TypeConfusion	Critical	GitHub Link to be added.
26	TypeConfusion	Critical	GitHub Link to be added.
27	TypeConfusion	Critical	GitHub Link to be added.
28	TypeConfusion	Critical	GitHub Link to be added.
29	TypeConfusion	Critical	GitHub Link to be added.
30	TypeConfusion	Critical	GitHub Link to be added.
31	TypeConfusion	Critical	GitHub Link to be added.
32	TypeConfusion	Critical	GitHub Link to be added.
33	TypeConfusion	Critical	GitHub Link to be added.
34	TypeConfusion	Critical	GitHub Link to be added.
35	TypeConfusion	Critical	GitHub Link to be added.
36	TypeConfusion	Critical	GitHub Link to be added.

**Issue: 0: IntegerFlow**

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/processor/set\_store\_index.rs:169:49: 169:61

```
169 offset_u - 1
170
```

- Code Context

Vulnerability at Line: 169

```
164         return
165         ↪ Err(MetaplexError::ExpectedAboveAuctionCacheToBeProvided.into());
166     }
167 }
168 if offset_u > 0 {
169     let below_key = &indexer.auction_caches[offset_u - 1];
170     // special case where you're at top of stack, there is no above
171     let cache_used_for_below = if offset_u ==
172     ↪ indexer.auction_caches.len() - 1 {
173         &above_cache
174     } else {
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
2     ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
3     fn processor::process_instruction() {
4         ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
5         fn processor::set_store_index::process_set_store_index() {
6             ↪ metaplex/program/src/processor/set_store_index.rs:22:1: 217:2 }
```

- description:
- link:
- alleviation:

## Issue: 1: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1538:35: 1540:59

```

1538 7 - order
1539     .checked_rem(8)
1540     .ok_or(MetaplexError::NumericalOverflowError)?
1541

```

- Code Context

Vulnerability at Line: 1538

```

1533     let u8_position = order
1534         .checked_div(8)
1535         .ok_or(MetaplexError::NumericalOverflowError)?
1536         .checked_add(offset)
1537         .ok_or(MetaplexError::NumericalOverflowError)?;
1538     let position_from_right = 7 - order
1539         .checked_rem(8)
1540         .ok_or(MetaplexError::NumericalOverflowError)?;
1541     let mask = u8::pow(2, position_from_right as u32);
1542
1543

```

- Call Stack

```

1  fn entrypoint::process_instruction() {
    ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2  fn processor::process_instruction() {
    ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
3  fn proces-
    ↪ sor::redeem_participation_bid::process_redeem_participation_bid() {
    ↪ meta-
    ↪ plex/program/src/processor/redeem_participation_bid.rs:235:1:
    ↪ 447:2 }

```

```
4      fn utils::common_redeem_checks() {  
5          ↪ metaplex/program/src/utils.rs:509:1: 681:2 }  
6          fn state::BidRedemptionTicket::check_ticket() {  
7              ↪ metaplex/program/src/state.rs:1476:5: 1520:6 }  
              fn  
              ↪ state::BidRedemptionTicket::get_index_and_mask() {  
              ↪ metaplex/program/src/state.rs:1522:5: 1544:6 }
```

- description:
- link:
- alleviation:

## Issue: 2: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/utils.rs:742:17: 742:59

```
742 1 + 9 + 32 + 1 + token_type_count as usize
743
```

- Code Context

Vulnerability at Line: 742

```
737         *program_id,
738         &bid_redemption_info,
739         &rent_info,
740         &system_info,
741         &payer_info,
742         1 + 9 + 32 + 1 + token_type_count as usize,
743         redemption_seeds,
744     )?;
745 }
746
747
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2   fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3     fn proces-
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-
  ↳ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
4     fn utils::common_redeem_finish() {
  ↳ metaplex/program/src/utils.rs:702:1: 776:2 }
```

5

- description:
- link:
- alleviation:

### Issue: 3: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1460:13: 1460:48

```
1460 offset += self.amount_type as usize
1461
```

- Code Context

Vulnerability at Line: 1460

```
1455     data[2] = self.length_type as u8;
1456     *array_mut_ref![data, 3, 4] = (self.amount_ranges.len() as
↪ u32).to_le_bytes();
1457     let mut offset: usize = 7;
1458     for range in &self.amount_ranges {
1459         write_amount_type(&mut data, self.amount_type, offset, range);
1460         offset += self.amount_type as usize;
1461         write_length_type(&mut data, self.length_type, offset, range);
1462         offset += self.length_type as usize;
1463     }
1464 }
1465
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
↪   metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2   fn processor::process_instruction() {
↪   metaplex/program/src/processor.rs:50:1: 169:2 }
3   fn proces-
↪   sor::validate_safety_deposit_box_v2::process_validate_safety_deposit_box_v2(
↪   meta-
↪   plex/program/src/processor/validate_safety_deposit_box_v2.rs:383:1:
↪   533:2 }
4   fn state::AuctionWinnerTokenTypeTracker::save() {
↪   metaplex/program/src/state.rs:1451:5: 1464:6 }
```



5

- description:
- link:
- alleviation:

## Issue: 4: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

/home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/arrayref-0.3.6/src/lib.rs:290:43:290:49

```
290 offset
291
```

- Code Context

– Function Definition:

```
887 fn write_length_type(
888     data: &mut RefMut<&mut [u8]>,
889     length_type: TupleNumericType,
890     offset: usize,
891     range: &AmountRange,
892 )
893
```

Vulnerability at Line: 890

```
887 fn write_length_type(
888     data: &mut RefMut<&mut [u8]>,
889     length_type: TupleNumericType,
890     offset: usize,
891     range: &AmountRange,
892 ) {
893     match length_type {
894         TupleNumericType::U8 => data[offset] = range.1 as u8,
895
```

Other Use Case for Variable: offset

```

894     TupleNumericType::U8 => data[offset] = range.1 as u8,

895     TupleNumericType::U16 => *array_mut_ref![data, offset, 2] =
    ↪ (range.1 as u16).to_le_bytes(),

896     TupleNumericType::U32 => *array_mut_ref![data, offset, 4] =
    ↪ (range.1 as u32).to_le_bytes(),

897     TupleNumericType::U64 => *array_mut_ref![data, offset, 8] =
    ↪ range.1.to_le_bytes(),

```

- Call Stack

```

1  fn entrypoint::process_instruction() {
    ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2  fn processor::process_instruction() {
    ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
3  fn proces-
    ↪ sor::validate_safety_deposit_box_v2::process_validate_safety_deposit_box_v2(
    ↪ meta-
    ↪ plex/program/src/processor/validate_safety_deposit_box_v2.rs:383:1:
    ↪ 533:2 }
4  fn state::AuctionWinnerTokenTypeTracker::save() {
    ↪ metaplex/program/src/state.rs:1451:5: 1464:6 }
5      fn state::write_length_type() {
    ↪ metaplex/program/src/state.rs:887:1: 900:2 }
6

```

- description:
- link:
- alleviation:

## Issue: 5: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/state.rs:906:15: 906:70

```
906 (self.amount_type as usize + self.length_type as usize)
907
```

- Code Context

Vulnerability at Line: 906

```
904 pub fn created_size(&self) -> usize {
905     return BASE_SAFETY_CONFIG_SIZE
906         + (self.amount_type as usize + self.length_type as usize) *
↪ self.amount_ranges.len();
907 }
908
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
↪ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
↪ sor::validate_safety_deposit_box_v2::process_validate_safety_deposit_box_v2(
↪ meta-
↪ plex/program/src/processor/validate_safety_deposit_box_v2.rs:383:1:
↪ 533:2 }
4 fn proces-
↪ sor::validate_safety_deposit_box_v2::make_safety_deposit_config() {
↪ meta-
↪ plex/program/src/processor/validate_safety_deposit_box_v2.rs:27:1:
↪ 67:2 }
5 fn state::SafetyDepositConfig::created_size() {
↪ metaplex/program/src/state.rs:904:5: 907:6 }
```

6

- description:
- link:
- alleviation:

## Issue: 6: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1182:13: 1182:48

```
1182 offset += self.amount_type as usize
1183
```

- Code Context

Vulnerability at Line: 1182

```
1177 *array_mut_ref![data, AMOUNT_RANGE_SIZE_POSITION, 4] =
1178     (self.amount_ranges.len() as u32).to_le_bytes();
1179 let mut offset: usize = AMOUNT_RANGE_FIRST_EL_POSITION;
1180 for range in &self.amount_ranges {
1181     write_amount_type(&mut data, self.amount_type, offset, range);
1182     offset += self.amount_type as usize;
1183     write_length_type(&mut data, self.length_type, offset, range);
1184     offset += self.length_type as usize;
1185 }
1186
1187
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
  ↳ sor::validate_safety_deposit_box_v2::process_validate_safety_deposit_box_v2(
  ↳ meta-
  ↳ plex/program/src/processor/validate_safety_deposit_box_v2.rs:383:1:
  ↳ 533:2 }
4 fn proces-
  ↳ sor::validate_safety_deposit_box_v2::make_safety_deposit_config() {
  ↳ meta-
  ↳ plex/program/src/processor/validate_safety_deposit_box_v2.rs:27:1:
  ↳ 67:2 }
```

```
5      fn state::SafetyDepositConfig::create() {  
6          ↪ metaplex/program/src/state.rs:1164:5: 1227:6 }
```

- description:
- link:
- alleviation:

## Issue: 7: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1278:15: 1278:92

```
1278 (self.amount_type as usize + self.length_type as usize) * range_size as
    ↳ usize
1279
```

- Code Context

Vulnerability at Line: 1278

```
1276 pub fn created_size(&self, range_size: u64) -> usize {
1277     return BASE_TRACKER_SIZE
1278         + (self.amount_type as usize + self.length_type as usize) *
    ↳ range_size as usize;
1279 }
1280
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
    ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
    ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
    ↳ sor::init_auction_manager_v2::process_init_auction_manager_v2() {
    ↳ metaplex/program/src/processor/init_auction_manager_v2.rs:97:1:
    ↳ 196:2 }
4 fn state::AuctionWinnerTokenTypeTracker::created_size() {
    ↳ metaplex/program/src/state.rs:1276:5: 1279:6 }
5
```

- description:



- link:
- alleviation:

## Issue: 8: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/auction/program/src/processor.rs:650:33:650:51

```
650 bids.len() - index
651
```

- Code Context

Vulnerability at Line: 650

```
646 pub fn amount(&self, index: usize) -> u64 {
647     match self {
648         BidState::EnglishAuction { bids, max } => {
649             if index >= 0 as usize && index < bids.len() {
650                 return bids[bids.len() - index - 1].1;
651             } else {
652                 return 0;
653             }
654         }
655     }
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn processor::empty_payment_account::process_empty_payment_account() {
  ↳ metaplex/program/src/processor/empty_payment_account.rs:212:1:
  ↳ 458:2 }
4 fn processor::empty_payment_account::calculate_owed_amount() {
  ↳ meta-
  ↳ plex/program/src/processor/empty_payment_account.rs:75:1:
  ↳ 210:2 }
```

5

```
fn mpl_auction::processor::BidState::amount(){//  
↳ /mnt/data/yifei/open/vrust/examples2/metaplex-  
↳ program-  
↳ library/auction/program/src/processor.rs:646:5:  
↳ 657:6 }
```

6

- description:
- link:
- alleviation:

## Issue: 9: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

metaplex/program/src/processor/empty\_payment\_account.rs:126:17: 126:64

```
126 (10000 - metadata.data.seller_fee_basis_points)
127
```

- Code Context

– Function Definition:

```
75 fn calculate_owed_amount(
76     auction_token_tracker_info: Option<&AccountInfo>,
77     safety_deposit_config_info: Option<&AccountInfo>,
78     auction_manager: &Box<dyn AuctionManager>,
79     auction: &AuctionData,
80     metadata: &Metadata,
81     winning_config_index: &Option<u8>,
82     winning_config_item_index: &Option<u8>,
83     creator_index: &Option<u8>,
84 ) -> Result<u64, ProgramError>
85
```

Vulnerability at Line: 126

```
121     }
122 }
123 None => {
124     if primary_sale_happened {
125         // during secondary sale, auctioneer gets whats left after
126         ↪ artists get their cut
127         (10000 - metadata.data.seller_fee_basis_points) as u128
128     } else {
129         // during primary sale, auctioneer (creator index not
130         ↪ provided)
```

```

129         // get none of the proceeds
130         0u128
131

```

- Call Stack

```

1  fn entrypoint::process_instruction(){//
    ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2  fn processor::process_instruction(){//
    ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3  fn proces-
    ↳ sor::empty_payment_account::process_empty_payment_account(){//
    ↳ metaplex/program/src/processor/empty_payment_account.rs:212:1:
    ↳ 458:2 }
4  fn processor::empty_payment_account::calculate_owed_amount(){//
    ↳ meta-
    ↳ plex/program/src/processor/empty_payment_account.rs:75:1:
    ↳ 210:2 }
5

```

- description:
- link:
- alleviation:

## Issue: 10: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account\_info.rs:66:11: 66:33

```
66 self.lamports.borrow()
```

```
67
```

- Code Context

Vulnerability at Line: 66

```
65 pub fn lamports(&self) -> u64 {
66     **self.lamports.borrow()
67 }
68
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2   fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3     fn processor::set_store::process_set_store_v2() {
  ↳ metaplex/program/src/processor/set_store.rs:122:1: 193:2 }
4       fn processor::set_store::set_store_logic() {
  ↳ metaplex/program/src/processor/set_store.rs:19:1: 88:2 }
5         fn utils::create_or_allocate_account_raw() {
  ↳ metaplex/program/src/utils.rs:212:1: 257:2 }
6           fn
  ↳ solana_program::account_info::AccountInfo::<'a>::lamports() {
  ↳ /home/yifei/.cargo/registry/src/github.com-
  ↳ 1ecc6299db9ec823/solana-program-
  ↳ 1.9.5/src/account_info.rs:65:5: 67:6
  ↳ }
7
```

- 
- description:
  - link:
  - alleviation:

## Issue: 11: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

metaplex/program/src/processor/set\_store.rs:86:27: 86:55

```
86 store_info.data.borrow_mut()
87
```

- Code Context

Vulnerability at Line: 86

```
81     store.token_metadata_program = *token_metadata_program_info.key;
82 }
83 if store.auction_program == solana_program::system_program::id() {
84     store.auction_program = *auction_program_info.key;
85 }
86 store.serialize(&mut *store_info.data.borrow_mut())?;
87 Ok(())
88 }
89
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2   fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3     fn processor::set_store::process_set_store_v2() {
  ↳ metaplex/program/src/processor/set_store.rs:122:1: 193:2 }
4       fn processor::set_store::set_store_logic() {
  ↳ metaplex/program/src/processor/set_store.rs:19:1: 88:2 }
5
```

- description:



- link:
- alleviation:

## Issue: 12: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

metaplex/program/src/state.rs:213:19: 213:40

```
213 account.data.borrow()
214
```

- Code Context

Vulnerability at Line: 213

```
212 pub fn get_auction_manager(account: &AccountInfo) -> Result<Box<dyn
    ↳ AuctionManager>, ProgramError> {
213     let version = account.data.borrow()[0];
214
215     // For some reason when converting Key to u8 here, it becomes
    ↳ unreachable. Use direct constant instead.
216     match version {
217         7 => return
    ↳ Ok(Box::new(AuctionManagerV1::from_account_info(account)?)),
218
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
    ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
    ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn processor::end_auction::process_end_auction() {
    ↳ metaplex/program/src/processor/end_auction.rs:43:1: 118:2 }
4 fn state::get_auction_manager() {
    ↳ metaplex/program/src/state.rs:212:1: 221:2 }
5
```

- description:

- link:
- alleviation:

## Issue: 13: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

metaplex/program/src/utlis.rs:540:22: 540:46

```
540 store_info.data.borrow()
541
```

- Code Context

Vulnerability at Line: 540

```
535     } = args;
536
537     let rent = &Rent::from_account_info(&rent_info)?;
538
539     let mut auction_manager: Box<dyn AuctionManager> =
540         ↪ get_auction_manager(auction_manager_info)?;
541     let store_data = store_info.data.borrow();
542     let cancelled: bool;
543
544     let auction_program = Pubkey::new_from_array(*array_ref![store_data, 2,
545         ↪ 32]);
546     let token_vault_program =
547         ↪ Pubkey::new_from_array(*array_ref![store_data, 34, 32]);
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
2     ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
3     fn processor::process_instruction() {
4         ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
5         fn proces-
6             ↪ sor::redeem_participation_bid::process_redeem_participation_bid() {
7             ↪ meta-
8             ↪ plex/program/src/processor/redeem_participation_bid.rs:235:1:
9             ↪ 447:2 }
```

```
4      fn utils::common_redeem_checks(){//  
5          ↪ metaplex/program/src/utils.rs:509:1: 681:2 }
```

- description:
- link:
- alleviation:

**Issue: 14: MissingKeyCheck**

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/auction/program/src/processor.rs:191:20:191:35

```
191 a.data.borrow()
192
```

- Code Context

– Function Definition:

```
190 fn find_bid_state_beginning(a: &AccountInfo) -> usize
191
```

Vulnerability at Line: 191

```
190 fn find_bid_state_beginning(a: &AccountInfo) -> usize {
191     let data = a.data.borrow();
192     let mut bid_state_beginning = 32 + 32;
193
194     for i in 0..4 {
195         // One for each unix timestamp
196     }
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-
  ↳ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
```

4  
5  
6  
7  
8

```
fn utils::common_redeem_checks(){//
    ↪ metaplex/program/src/utils.rs:509:1: 681:2 }
fn utils::calculate_win_index(){//
    ↪ metaplex/program/src/utils.rs:422:1: 471:2 }
fn
    ↪ mpl_auction::processor::AuctionData::get_is_winner(){//
    ↪ /mnt/data/yifei/open/vrust/examples2/metaplex-
    ↪ program-
    ↪ library/auction/program/src/processor.rs:221:5:
    ↪ 252:6 }
fn
    ↪ mpl_auction::processor::AuctionData::find_bid_state_begi
    ↪ /mnt/data/yifei/open/vrust/examples2/metaplex-
    ↪ program-
    ↪ library/auction/program/src/processor.rs:190:5:
    ↪ 207:6 }
```

- description:
- link:
- alleviation:

**Issue: 15: MissingKeyCheck**

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/auction/program/src/processor.rs:223:20: 223:35

```
223 a.data.borrow()
224
```

- Code Context

Vulnerability at Line: 223

```
221 pub fn get_is_winner(a: &AccountInfo, key: &Pubkey) -> Option<usize> {
222     let bid_state_beginning = AuctionData::find_bid_state_beginning(a);
223     let data = a.data.borrow();
224     let as_bytes = key.to_bytes();
225     let (bid_state_beginning, num_elements, max) =
226     ↪ AuctionData::get_vec_info(a);
227     for idx in 0..std::cmp::min(num_elements, max) {
228         match AuctionData::get_winner_at_inner(
```

Other Use Case for Variable: a.data.borrow()

```
228         &a.data.borrow(),
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
  ↪ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↪ meta-
  ↪ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↪ 447:2 }
```



```

4      fn utils::common_redeem_checks() { //
      ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5      fn utils::calculate_win_index() { //
      ↪  metaplex/program/src/utils.rs:422:1: 471:2 }
6      fn
      ↪  mpl_auction::processor::AuctionData::get_is_winner() { //
      ↪  /mnt/data/yifei/open/vrust/examples2/metaplex-
      ↪  program-
      ↪  library/auction/program/src/processor.rs:221:5:
      ↪  252:6 }
7

```

- description:
- link:
- alleviation:

**Issue: 16: MissingKeyCheck**

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/auction/program/src/processor.rs:211:20: 211:35

```
211 a.data.borrow()
212
```

- Code Context

– Function Definition:

```
209 fn get_vec_info(a: &AccountInfo) -> (usize, usize, usize)
210
```

Vulnerability at Line: 211

```
209 fn get_vec_info(a: &AccountInfo) -> (usize, usize, usize) {
210     let bid_state_beginning = AuctionData::find_bid_state_beginning(a);
211     let data = a.data.borrow();
212
213     let num_elements_data = array_ref![data, bid_state_beginning - 4,
        ↪ 4];
214     let num_elements = u32::from_le_bytes(*num_elements_data) as usize;
215     let max_data = array_ref![data, bid_state_beginning + BID_LENGTH *
        ↪ num_elements, 8];
216
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
    ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
    ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
```

```

3      fn proces-
      ↪ sor::redeem_participation_bid::process_redeem_participation_bid() { //
      ↪ meta-
      ↪ plex/program/src/processor/redeem_participation_bid.rs:235:1:
      ↪ 447:2 }
4      fn utils::common_redeem_checks() { //
      ↪ metaplex/program/src/utils.rs:509:1: 681:2 }
5      fn utils::calculate_win_index() { //
      ↪ metaplex/program/src/utils.rs:422:1: 471:2 }
6      fn
      ↪ mpl_auction::processor::AuctionData::get_is_winner() { //
      ↪ /mnt/data/yifei/open/vrust/examples2/metaplex-
      ↪ program-
      ↪ library/auction/program/src/processor.rs:221:5:
      ↪ 252:6 }
7      fn
      ↪ mpl_auction::processor::AuctionData::get_vec_info() { //
      ↪ /mnt/data/yifei/open/vrust/examples2/metaplex-
      ↪ program-
      ↪ library/auction/program/src/processor.rs:209:5:
      ↪ 219:6 }
8

```

- description:
- link:
- alleviation:

## Issue: 17: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/auction/program/src/processor.rs:257:14:257:29

```

257 a.data.borrow()
258

```

- Code Context

Vulnerability at Line: 257

```

254 pub fn get_winner_at(a: &AccountInfo, idx: usize) -> Option<Pubkey> {
255     let (bid_state_beginning, num_elements, max) =
        ↳ AuctionData::get_vec_info(a);
256     match AuctionData::get_winner_at_inner(
257         &a.data.borrow(),
258         idx,
259         bid_state_beginning,
260         num_elements,
261         max,
262

```

- Call Stack

```

1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-
  ↳ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
4 fn utils::common_redeem_checks() {
  ↳ metaplex/program/src/utils.rs:509:1: 681:2 }

```

```

5      fn utils::calculate_win_index(){//
      ↪  metaplex/program/src/utis.rs:422:1: 471:2 }
6      fn
      ↪  mpl_auction::processor::AuctionData::get_winner_at(){//
      ↪  /mnt/data/yifei/open/vrust/examples2/metaplex-
      ↪  program-
      ↪  library/auction/program/src/processor.rs:254:5:
      ↪  266:6 }
7

```

- description:
- link:
- alleviation:

**Issue: 18: MissingKeyCheck**

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

metaplex/program/src/state.rs:910:20: 910:35

```
910 a.data.borrow()
911
```

- Code Context

Vulnerability at Line: 910

```
909 pub fn get_order(a: &AccountInfo) -> u64 {
910     let data = a.data.borrow();
911     return u64::from_le_bytes(*array_ref![data, ORDER_POSITION, 8]);
912 }
913
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3   fn process_redeem_participation_bid() {
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
4   fn utils::common_redeem_checks() {
  ↳ metaplex/program/src/utls.rs:509:1: 681:2 }
5     fn state::BidRedemptionTicket::check_ticket() {
  ↳ metaplex/program/src/state.rs:1476:5: 1520:6 }
6     fn state::SafetyDepositConfig::get_order() {
  ↳ metaplex/program/src/state.rs:909:5: 912:6 }
7
```

- description:
- link:
- alleviation:

## Issue: 19: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/auction/program/src/processor.rs:168:20:168:35

```
168 a.data.borrow()
169
```

- Code Context

Vulnerability at Line: 168

```
167 pub fn get_token_mint(a: &AccountInfo) -> Pubkey {
168     let data = a.data.borrow();
169     let token_mint_data = array_ref![data, 32, 32];
170     Pubkey::new_from_array(*token_mint_data)
171 }
172
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-
  ↳ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
4 fn mpl_auction::processor::AuctionData::get_token_mint() {
  ↳ /mnt/data/yifei/open/vrust/examples2/metaplex-program-
  ↳ library/auction/program/src/processor.rs:167:5: 171:6
  ↳ }
5
```



- description:
- link:
- alleviation:

## Issue: 20: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account\_info.rs:102:9:103:26

```

102 self.data
103     .try_borrow()
104

```

- Code Context

Vulnerability at Line: 102

```

101 pub fn try_borrow_data(&self) -> Result<Ref<&mut [u8]>, ProgramError> {
102     self.data
103         .try_borrow()
104         .map_err(|_| ProgramError::AccountBorrowFailed)
105 }
106

```

- Call Stack

```

1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3 fn proces-
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-
  ↳ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
4 fn
  ↳ mpl_token_metadata::utils::get_supply_off_master_edition() {
  ↳ /home/yifei/.cargo/registry/src/github.com-
  ↳ 1ecc6299db9ec823/mpl-token-metadata-
  ↳ 1.1.0/src/utils.rs:483:1: 491:2
  ↳ }

```

5

**fn**

```
↳ solana_program::account_info::AccountInfo::<'a>::try_borrow_data
↳ /home/yifei/.cargo/registry/src/github.com-
↳ 1ecc6299db9ec823/solana-program-
↳ 1.9.5/src/account_info.rs:101:5: 105:6
↳ }
```

6

- description:
- link:
- alleviation:

## Issue: 21: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

metaplex/program/src/processor/redeem\_printing\_v2\_bid.rs:107:25: 107:60

```
107 metadata_account_info.data.borrow()
108
```

- Code Context

Vulnerability at Line: 107

```
102     rent_info: &AccountInfo<'a>,
103     system_info: &AccountInfo<'a>,
104     master_edition_account_info: &AccountInfo<'a>,
105     expected_redemptions: u64,
106 ) -> Result<u64, ProgramError> {
107     let metadata_data = metadata_account_info.data.borrow();
108     let metadata_mint = Pubkey::new_from_array(*array_ref![metadata_data,
109         ↪ 33, 32]);
110
111     let bump = assert_derivation(
112         program_id,
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↪ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2 fn processor::process_instruction() {
  ↪ metaplex/program/src/processor.rs:50:1: 169:2 }
3     fn proces-
  ↪ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↪ meta-
  ↪ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↪ 447:2 }
4     fn processor::redeem_participation_bid::v2_validation() {
  ↪ meta-
  ↪ plex/program/src/processor/redeem_participation_bid.rs:65:1:
  ↪ 129:2 }
```

5

```
fn proces-  
↳ sor::redeem_printing_v2_bid::create_or_update_prize_tracking() {/  
↳ meta-  
↳ plex/program/src/processor/redeem_printing_v2_bid.rs:96:1:  
↳ 165:2 }
```

6

- description:
- link:
- alleviation:

**Issue: 22: MissingKeyCheck**

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/mnt/data/yifei/open/vrust/examples2/metaplex-program-library/token-vault/program/src/state.rs:71:16: 71:31

```
71 a.data.borrow()
72
```

- Code Context

Vulnerability at Line: 71

```
70 pub fn get_token_type_count(a: &AccountInfo) -> u8 {
71     return a.data.borrow()[194];
72 }
73
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↳ metaplex/program/src/entrypoint.rs:14:1: 25:2 }
2   fn processor::process_instruction() {
  ↳ metaplex/program/src/processor.rs:50:1: 169:2 }
3     fn proces-
  ↳ sor::redeem_participation_bid::process_redeem_participation_bid() {
  ↳ meta-
  ↳ plex/program/src/processor/redeem_participation_bid.rs:235:1:
  ↳ 447:2 }
4     fn utils::common_redeem_finish() {
  ↳ metaplex/program/src/utils.rs:702:1: 776:2 }
5       fn
  ↳ mpl_token_vault::state::Vault::get_token_type_count() {
  ↳ /mnt/data/yifei/open/vrust/examples2/metaplex-
  ↳ program-library/token-
  ↳ vault/program/src/state.rs:70:5: 72:6
  ↳ }
```

6

- description:
- link:
- alleviation:

## Issue: 23: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/processor/redeem\_participation\_bid.rs:25:1: 27:2

```

25 struct LegacyAccounts<'a> {
26     pub participation_printing_holding_account_info: &'a AccountInfo<'a>,
27 }
28 metaplex/program/src/state.rs:558:1: 566:2
29     pub struct ParticipationStateV2 {
30         /// We have this variable below to keep track in the case of the
31         ↪ participation NFTs, whose
32         /// income will trickle in over time, how much the artists have in the
33         ↪ escrow account and
34         /// how much would/should be owed to them if they try to claim it
35         ↪ relative to the winning bids.
36         /// It's abit tougher than a straightforward bid which has a price
37         ↪ attached to it, because
38         /// there are many bids of differing amounts (in the case of
39         ↪ GivenForBidPrice) and they dont all
40         /// come in at one time, so this little ledger here keeps track.
41         pub collected_to_accept_payment: u64,
42     }
43 metaplex/program/src/instruction.rs:52:1: 55:2
44     pub struct RedeemPrintingV2BidArgs {
45         pub edition_offset: u64,
46         pub win_index: u64,
47     }
48 metaplex/program/src/instruction.rs:82:1: 85:2
49     pub struct SetStoreIndexArgs {
50         pub page: u64,
51         pub offset: u64,
52     }
53 metaplex/program/src/state.rs:805:1: 805:42
54     pub struct AmountRange(pub u64, pub u64);
55 metaplex/program/src/state.rs:118:1: 122:2

```



```

51     pub struct CommonWinningIndexReturn {
52     pub amount: u64,
53     pub winning_config_type: WinningConfigType,
54     pub winning_config_item_index: Option<usize>,
55 }
56 metaplex/program/src/state.rs:124:1: 128:2
57     pub struct PrintingV2CalculationCheckReturn {
58     pub expected_redemptions: u64,
59     pub winning_config_type: WinningConfigType,
60     pub winning_config_item_index: Option<usize>,
61 }
62 metaplex/program/src/state.rs:849:1: 853:2
63     pub struct AmountCumulativeReturn {
64     pub amount: u64,
65     pub cumulative_amount: u64,
66     pub total_amount: u64,
67 }
68 metaplex/program/src/state.rs:101:1: 106:2
69     pub struct CommonWinningIndexChecks<'a> {
70     pub safety_deposit_info: &'a AccountInfo<'a>,
71     pub winning_index: usize,
72     pub auction_manager_v1_ignore_claim: bool,
73     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
74 }
75 metaplex/program/src/deprecated_state.rs:557:1: 575:2
76     pub struct ParticipationStateV1 {
77     /// We have this variable below to keep track in the case of the
78     ↪ participation NFTs, whose
79     /// income will trickle in over time, how much the artists have in the
80     ↪ escrow account and
81     /// how much would/should be owed to them if they try to claim it
82     ↪ relative to the winning bids.
83     /// It's abit tougher than a straightforward bid which has a price
84     ↪ attached to it, because
85     /// there are many bids of differing amounts (in the case of
86     ↪ GivenForBidPrice) and they dont all
87     /// come in at one time, so this little ledger here keeps track.
88     pub collected_to_accept_payment: u64,
89
90     /// Record of primary sale or not at time of auction creation, set
91     ↪ during validation step
92     pub primary_sale_happened: bool,

```

```
87
88     pub validated: bool,
89
90     /// NOTE: DEPRECATED.
91     /// An account for printing authorization tokens that are made with the
92         ↪ one time use token
93     /// after the auction ends. Provided during validation step.
94     pub printing_authorization_token_account: Option<Pubkey>,
95 }
96 metaplex/program/src/state.rs:108:1: 116:2
97     pub struct PrintingV2CalculationChecks<'a> {
98     pub safety_deposit_info: &'a AccountInfo<'a>,
99     pub winning_index: usize,
100     pub auction_manager_v1_ignore_claim: bool,
101     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
102     pub short_circuit_total: bool,
103     pub edition_offset: u64,
104     pub winners: usize,
105 }
106 metaplex/program/src/processor/redeem_participation_bid.rs:29:1: 39:2
107     struct V2Accounts<'a> {
108     pub prize_tracking_ticket_info: &'a AccountInfo<'a>,
109     pub new_metadata_account_info: &'a AccountInfo<'a>,
110     pub new_edition_account_info: &'a AccountInfo<'a>,
111     pub master_edition_account_info: &'a AccountInfo<'a>,
112     pub mint_info: &'a AccountInfo<'a>,
113     pub edition_marker_info: &'a AccountInfo<'a>,
114     pub mint_authority_info: &'a AccountInfo<'a>,
115     pub metadata_account_info: &'a AccountInfo<'a>,
116     pub auction_extended_info: &'a AccountInfo<'a>,
117 }
118 metaplex/program/src/utils.rs:683:1: 700:2
119     pub struct CommonRedeemFinishArgs<'a> {
120     pub program_id: &'a Pubkey,
121     pub auction_manager: Box<dyn AuctionManager>,
122     pub auction_manager_info: &'a AccountInfo<'a>,
123     pub bidder_metadata_info: &'a AccountInfo<'a>,
124     pub rent_info: &'a AccountInfo<'a>,
125     pub system_info: &'a AccountInfo<'a>,
126     pub payer_info: &'a AccountInfo<'a>,
127     pub bid_redemption_info: &'a AccountInfo<'a>,
128     pub vault_info: &'a AccountInfo<'a>,
```

```
128     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
129     pub winning_index: Option<usize>,
130     pub redemption_bump_seed: u8,
131     pub bid_redeemed: bool,
132     pub participation_redeemed: bool,
133     pub winning_item_index: Option<usize>,
134     pub overwrite_win_index: Option<usize>,
135 }
136 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:185:1:
137 ↪ 203:2
138     pub struct SupplyLogicCheckArgs<'a, 'b> {
139     pub program_id: &'a Pubkey,
140     pub auction_manager_info: &'a AccountInfo<'a>,
141     pub metadata_info: &'a AccountInfo<'a>,
142     pub edition_info: &'a AccountInfo<'a>,
143     pub metadata_authority_info: &'a AccountInfo<'a>,
144     pub original_authority_lookup_info: &'a AccountInfo<'a>,
145     pub rent_info: &'a AccountInfo<'a>,
146     pub system_info: &'a AccountInfo<'a>,
147     pub payer_info: &'a AccountInfo<'a>,
148     pub token_metadata_program_info: &'a AccountInfo<'a>,
149     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
150     pub auction_manager: &'b dyn AuctionManager,
151     pub winning_config_type: &'b WinningConfigType,
152     pub metadata: &'b Metadata,
153     pub safety_deposit: &'b SafetyDepositBox,
154     pub store: &'b Store,
155     pub total_amount_requested: u64,
156 }
157 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:69:1: 89:2
158     pub struct CommonCheckArgs<'a, 'b> {
159     pub program_id: &'a Pubkey,
160     pub auction_manager_info: &'a AccountInfo<'a>,
161     pub metadata_info: &'a AccountInfo<'a>,
162     pub original_authority_lookup_info: &'a AccountInfo<'a>,
163     pub whitelisted_creator_info: &'a AccountInfo<'a>,
164     pub safety_deposit_info: &'a AccountInfo<'a>,
165     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
166     pub edition_info: &'a AccountInfo<'a>,
167     pub vault_info: &'a AccountInfo<'a>,
168     pub mint_info: &'a AccountInfo<'a>,
169     pub token_metadata_program_info: &'a AccountInfo<'a>,
```

```
169     pub auction_manager_store_info: &'a AccountInfo<'a>,
170     pub authority_info: &'a AccountInfo<'a>,
171     pub store: &'b Store,
172     pub auction_manager: &'b dyn AuctionManager,
173     pub metadata: &'b Metadata,
174     pub safety_deposit: &'b SafetyDepositBox,
175     pub vault: &'b Vault,
176     pub winning_config_type: &'b WinningConfigType,
177 }
178 metaplex/program/src/utils.rs:389:1: 420:2
179     pub struct CommonRedeemCheckArgs<'a> {
180     pub program_id: &'a Pubkey,
181     pub auction_manager_info: &'a AccountInfo<'a>,
182     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
183     pub destination_info: &'a AccountInfo<'a>,
184     pub bid_redemption_info: &'a AccountInfo<'a>,
185     pub safety_deposit_info: &'a AccountInfo<'a>,
186     pub vault_info: &'a AccountInfo<'a>,
187     pub auction_info: &'a AccountInfo<'a>,
188     pub auction_extended_info: Option<&'a AccountInfo<'a>>,
189     pub bidder_metadata_info: &'a AccountInfo<'a>,
190     pub bidder_info: &'a AccountInfo<'a>,
191     pub token_program_info: &'a AccountInfo<'a>,
192     pub token_vault_program_info: &'a AccountInfo<'a>,
193     pub token_metadata_program_info: &'a AccountInfo<'a>,
194     pub store_info: &'a AccountInfo<'a>,
195     pub rent_info: &'a AccountInfo<'a>,
196     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
197     pub is_participation: bool,
198     // If this is being called by the auctioneer to pull prizes out they
199     //   ↳ overwrite the win index
200     // they would normally get if they themselves bid for whatever win
201     //   ↳ index they choose.
202     pub overwrite_win_index: Option<usize>,
203     // In newer endpoints, to conserve CPU and make way for 10,000 person
204     //   ↳ auctions,
205     // client must specify win index and then we simply check if the
206     //   ↳ address matches for O(1) lookup vs O(n)
207     // scan. This is an option so older actions which rely on the O(n)
208     //   ↳ lookup because we can't change their call structure
209     // can continue to work.
210     pub user_provided_win_index: Option<Option<usize>>,
```

```
206     pub assert_bidder_signer: bool,  
207     // For printing v2, the edition pda is what essentially forms a  
208     ↪ backstop for bad bidders. We do not need this additional  
209     // check which isn't accurate anyway when one winning config item has  
210     ↪ an amount > 1.  
211     pub ignore_bid_redeemed_item_check: bool,  
212 }
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 24: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/deprecated\_state.rs:600:1: 604:2

```

600 pub struct WinningConfig {
601     // For now these are just array-of-array proxies but wanted to make
602     // ↳ them first class
603     // structs in case we want to attach other top level metadata someday.
604     pub items: Vec<WinningConfigItem>,
605 }
606 metaplex/program/src/instruction.rs:75:1: 79:2
607 pub struct EndAuctionArgs {
608     /// If the auction was blinded, a revealing price must be specified to
609     // ↳ release the auction
610     /// winnings.
611     pub reveal: Option<(u64, u64)>,
612 }
613 metaplex/program/src/deprecated_state.rs:545:1: 553:2
614 pub struct AuctionManagerSettingsV1 {
615     /// The safety deposit box index in the vault containing the winning
616     // ↳ items, in order of place
617     /// The same index can appear multiple times if that index contains n
618     // ↳ tokens for n appearances (this will be checked)
619     pub winning_configs: Vec<WinningConfig>,
620
621     /// The participation config is separated because it is structurally a
622     // ↳ bit different,
623     /// having different options and also because it has no real "winning
624     // ↳ place" in the array.
625     pub participation_config: Option<ParticipationConfigV1>,
626 }
627 metaplex/program/src/deprecated_state.rs:608:1: 612:2
628 pub struct WinningConfigState {
629     pub items: Vec<WinningConfigStateItem>,
630     /// Ticked to true when money is pushed to accept_payment account from
631     // ↳ auction bidding pot

```

```
625     pub money_pushed_to_accept_payment: bool,  
626 }  
627
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 25: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/instruction.rs:13:1: 15:2

```

13 pub struct SetStoreArgs {
14     pub public: bool,
15 }
16 metaplex/program/src/instruction.rs:24:1: 26:2
17     pub struct SetWhitelistedCreatorArgs {
18         pub activated: bool,
19     }
20 metaplex/program/src/deprecated_state.rs:624:1: 629:2
21     pub struct WinningConfigStateItem {
22         /// Record of primary sale or not at time of auction creation, set
23         ↳ during validation step
24         pub primary_sale_happened: bool,
25         /// Ticked to true when a prize is claimed by person who won it
26         pub claimed: bool,
27     }
28 metaplex/program/src/instruction.rs:18:1: 21:2
29     pub struct SetStoreV2Args {
30         pub public: bool,
31         pub settings_uri: Option<String>,
32     }
33 metaplex/program/src/instruction.rs:46:1: 49:2
34     pub struct RedeemUnusedWinningConfigItemsAsAuctioneerArgs {
35         pub winning_config_item_index: u8,
36         pub proxy_call: ProxyCallAddress,
37     }
38 metaplex/program/src/deprecated_state.rs:616:1: 620:2
39     pub struct WinningConfigItem {
40         pub safety_deposit_box_index: u8,
41         pub amount: u8,
42         pub winning_config_type: WinningConfigType,
43     }

```



```
43 metaplex/program/src/utils.rs:380:1: 387:2
44     pub struct CommonRedeemReturn {
45     pub redemption_bump_seed: u8,
46     pub auction_manager: Box<dyn AuctionManager>,
47     pub cancelled: bool,
48     pub rent: Rent,
49     pub win_index: Option<usize>,
50     pub token_metadata_program: Pubkey,
51 }
52
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 26: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/instruction.rs:24:1: 26:2

```

24 pub struct SetWhitelistedCreatorArgs {
25     pub activated: bool,
26 }
27 metaplex/program/src/deprecated_state.rs:624:1: 629:2
28     pub struct WinningConfigStateItem {
29         /// Record of primary sale or not at time of auction creation, set
30         ↳ during validation step
31         pub primary_sale_happened: bool,
32         /// Ticked to true when a prize is claimed by person who won it
33         pub claimed: bool,
34 }
35 metaplex/program/src/instruction.rs:18:1: 21:2
36     pub struct SetStoreV2Args {
37         pub public: bool,
38         pub settings_uri: Option<String>,
39 }
40 metaplex/program/src/instruction.rs:46:1: 49:2
41     pub struct RedeemUnusedWinningConfigItemsAsAuctioneerArgs {
42         pub winning_config_item_index: u8,
43         pub proxy_call: ProxyCallAddress,
44 }
45 metaplex/program/src/deprecated_state.rs:616:1: 620:2
46     pub struct WinningConfigItem {
47         pub safety_deposit_box_index: u8,
48         pub amount: u8,
49         pub winning_config_type: WinningConfigType,
50 }
51 metaplex/program/src/utils.rs:380:1: 387:2
52     pub struct CommonRedeemReturn {
53         pub redemption_bump_seed: u8,
54         pub auction_manager: Box<dyn AuctionManager>,

```

```
54     pub cancelled: bool,  
55     pub rent: Rent,  
56     pub win_index: Option<usize>,  
57     pub token_metadata_program: Pubkey,  
58 }  
59
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 27: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/instruction.rs:75:1: 79:2

```

75 pub struct EndAuctionArgs {
76     /// If the auction was blinded, a revealing price must be specified to
77     ↪ release the auction
78     /// winnings.
79     pub reveal: Option<(u64, u64)>,
80 }
81 metaplex/program/src/deprecated_state.rs:545:1: 553:2
82 pub struct AuctionManagerSettingsV1 {
83     /// The safety deposit box index in the vault containing the winning
84     ↪ items, in order of place
85     /// The same index can appear multiple times if that index contains n
86     ↪ tokens for n appearances (this will be checked)
87     pub winning_configs: Vec<WinningConfig>,
88
89     /// The participation config is separated because it is structurally a
90     ↪ bit different,
91     /// having different options and also because it has no real "winning
92     ↪ place" in the array.
93     pub participation_config: Option<ParticipationConfigV1>,
94 }
95 metaplex/program/src/deprecated_state.rs:608:1: 612:2
96 pub struct WinningConfigState {
97     pub items: Vec<WinningConfigStateItem>,
98     /// Ticked to true when money is pushed to accept_payment account from
99     ↪ auction bidding pot
100     pub money_pushed_to_accept_payment: bool,
101 }

```

- Call Stack

# 1 UnResolved

- description:
- link:
- alleviation:

## Issue: 28: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/state.rs:558:1: 566:2

```

558 pub struct ParticipationStateV2 {
559     /// We have this variable below to keep track in the case of the
560     ↪ participation NFTs, whose
561     /// income will trickle in over time, how much the artists have in the
562     ↪ escrow account and
563     /// how much would/should be owed to them if they try to claim it
564     ↪ relative to the winning bids.
565     /// It's abit tougher than a straightforward bid which has a price
566     ↪ attached to it, because
567     /// there are many bids of differing amounts (in the case of
568     ↪ GivenForBidPrice) and they dont all
569     /// come in at one time, so this little ledger here keeps track.
570     pub collected_to_accept_payment: u64,
571 }
572 metaplex/program/src/instruction.rs:52:1: 55:2
573 pub struct RedeemPrintingV2BidArgs {
574     pub edition_offset: u64,
575     pub win_index: u64,
576 }
577 metaplex/program/src/instruction.rs:82:1: 85:2
578 pub struct SetStoreIndexArgs {
579     pub page: u64,
580     pub offset: u64,
581 }
582 metaplex/program/src/state.rs:805:1: 805:42
583 pub struct AmountRange(pub u64, pub u64);
584 metaplex/program/src/state.rs:118:1: 122:2
585 pub struct CommonWinningIndexReturn {
586     pub amount: u64,
587     pub winning_config_type: WinningConfigType,
588     pub winning_config_item_index: Option<usize>,

```

```
584 }
585 metaplex/program/src/state.rs:124:1: 128:2
586     pub struct PrintingV2CalculationCheckReturn {
587     pub expected_redemptions: u64,
588     pub winning_config_type: WinningConfigType,
589     pub winning_config_item_index: Option<usize>,
590 }
591 metaplex/program/src/state.rs:849:1: 853:2
592     pub struct AmountCumulativeReturn {
593     pub amount: u64,
594     pub cumulative_amount: u64,
595     pub total_amount: u64,
596 }
597 metaplex/program/src/state.rs:101:1: 106:2
598     pub struct CommonWinningIndexChecks<'a> {
599     pub safety_deposit_info: &'a AccountInfo<'a>,
600     pub winning_index: usize,
601     pub auction_manager_v1_ignore_claim: bool,
602     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
603 }
604 metaplex/program/src/deprecated_state.rs:557:1: 575:2
605     pub struct ParticipationStateV1 {
606     /// We have this variable below to keep track in the case of the
607     ↪ participation NFTs, whose
608     /// income will trickle in over time, how much the artists have in the
609     ↪ escrow account and
610     /// how much would/should be owed to them if they try to claim it
611     ↪ relative to the winning bids.
612     /// It's abit tougher than a straightforward bid which has a price
613     ↪ attached to it, because
614     /// there are many bids of differing amounts (in the case of
615     ↪ GivenForBidPrice) and they dont all
616     /// come in at one time, so this little ledger here keeps track.
617     pub collected_to_accept_payment: u64,
618
619     /// Record of primary sale or not at time of auction creation, set
620     ↪ during validation step
621     pub primary_sale_happened: bool,
622
623     pub validated: bool,
624
625     /// NOTE: DEPRECATED.
```

```
620    /// An account for printing authorization tokens that are made with the
621    ↪ one time use token
622    /// after the auction ends. Provided during validation step.
623    pub printing_authorization_token_account: Option<Pubkey>,
624 }
625 metaplex/program/src/state.rs:108:1: 116:2
626     pub struct PrintingV2CalculationChecks<'a> {
627     pub safety_deposit_info: &'a AccountInfo<'a>,
628     pub winning_index: usize,
629     pub auction_manager_v1_ignore_claim: bool,
630     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
631     pub short_circuit_total: bool,
632     pub edition_offset: u64,
633     pub winners: usize,
634 }
635 metaplex/program/src/processor/redeem_participation_bid.rs:29:1: 39:2
636     struct V2Accounts<'a> {
637     pub prize_tracking_ticket_info: &'a AccountInfo<'a>,
638     pub new_metadata_account_info: &'a AccountInfo<'a>,
639     pub new_edition_account_info: &'a AccountInfo<'a>,
640     pub master_edition_account_info: &'a AccountInfo<'a>,
641     pub mint_info: &'a AccountInfo<'a>,
642     pub edition_marker_info: &'a AccountInfo<'a>,
643     pub mint_authority_info: &'a AccountInfo<'a>,
644     pub metadata_account_info: &'a AccountInfo<'a>,
645     pub auction_extended_info: &'a AccountInfo<'a>,
646 }
647 metaplex/program/src/utils.rs:683:1: 700:2
648     pub struct CommonRedeemFinishArgs<'a> {
649     pub program_id: &'a Pubkey,
650     pub auction_manager: Box<dyn AuctionManager>,
651     pub auction_manager_info: &'a AccountInfo<'a>,
652     pub bidder_metadata_info: &'a AccountInfo<'a>,
653     pub rent_info: &'a AccountInfo<'a>,
654     pub system_info: &'a AccountInfo<'a>,
655     pub payer_info: &'a AccountInfo<'a>,
656     pub bid_redemption_info: &'a AccountInfo<'a>,
657     pub vault_info: &'a AccountInfo<'a>,
658     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
659     pub winning_index: Option<usize>,
660     pub redemption_bump_seed: u8,
661     pub bid_redeemed: bool,
```



```
661     pub participation_redeemed: bool,
662     pub winning_item_index: Option<usize>,
663     pub overwrite_win_index: Option<usize>,
664 }
665 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:185:1:
666 ↪ 203:2
667     pub struct SupplyLogicCheckArgs<'a, 'b> {
668     pub program_id: &'a Pubkey,
669     pub auction_manager_info: &'a AccountInfo<'a>,
670     pub metadata_info: &'a AccountInfo<'a>,
671     pub edition_info: &'a AccountInfo<'a>,
672     pub metadata_authority_info: &'a AccountInfo<'a>,
673     pub original_authority_lookup_info: &'a AccountInfo<'a>,
674     pub rent_info: &'a AccountInfo<'a>,
675     pub system_info: &'a AccountInfo<'a>,
676     pub payer_info: &'a AccountInfo<'a>,
677     pub token_metadata_program_info: &'a AccountInfo<'a>,
678     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
679     pub auction_manager: &'b dyn AuctionManager,
680     pub winning_config_type: &'b WinningConfigType,
681     pub metadata: &'b Metadata,
682     pub safety_deposit: &'b SafetyDepositBox,
683     pub store: &'b Store,
684     pub total_amount_requested: u64,
685 }
686 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:69:1: 89:2
687     pub struct CommonCheckArgs<'a, 'b> {
688     pub program_id: &'a Pubkey,
689     pub auction_manager_info: &'a AccountInfo<'a>,
690     pub metadata_info: &'a AccountInfo<'a>,
691     pub original_authority_lookup_info: &'a AccountInfo<'a>,
692     pub whitelisted_creator_info: &'a AccountInfo<'a>,
693     pub safety_deposit_info: &'a AccountInfo<'a>,
694     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
695     pub edition_info: &'a AccountInfo<'a>,
696     pub vault_info: &'a AccountInfo<'a>,
697     pub mint_info: &'a AccountInfo<'a>,
698     pub token_metadata_program_info: &'a AccountInfo<'a>,
699     pub auction_manager_store_info: &'a AccountInfo<'a>,
700     pub authority_info: &'a AccountInfo<'a>,
701     pub store: &'b Store,
702     pub auction_manager: &'b dyn AuctionManager,
```

```

702     pub metadata: &'b Metadata,
703     pub safety_deposit: &'b SafetyDepositBox,
704     pub vault: &'b Vault,
705     pub winning_config_type: &'b WinningConfigType,
706 }
707 metaplex/program/src/utils.rs:389:1: 420:2
708     pub struct CommonRedeemCheckArgs<'a> {
709     pub program_id: &'a Pubkey,
710     pub auction_manager_info: &'a AccountInfo<'a>,
711     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
712     pub destination_info: &'a AccountInfo<'a>,
713     pub bid_redemption_info: &'a AccountInfo<'a>,
714     pub safety_deposit_info: &'a AccountInfo<'a>,
715     pub vault_info: &'a AccountInfo<'a>,
716     pub auction_info: &'a AccountInfo<'a>,
717     pub auction_extended_info: Option<&'a AccountInfo<'a>>,
718     pub bidder_metadata_info: &'a AccountInfo<'a>,
719     pub bidder_info: &'a AccountInfo<'a>,
720     pub token_program_info: &'a AccountInfo<'a>,
721     pub token_vault_program_info: &'a AccountInfo<'a>,
722     pub token_metadata_program_info: &'a AccountInfo<'a>,
723     pub store_info: &'a AccountInfo<'a>,
724     pub rent_info: &'a AccountInfo<'a>,
725     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
726     pub is_participation: bool,
727     // If this is being called by the auctioneer to pull prizes out they
728     ↳ overwrite the win index
729     // they would normally get if they themselves bid for whatever win
730     ↳ index they choose.
731     pub overwrite_win_index: Option<usize>,
732     // In newer endpoints, to conserve CPU and make way for 10,000 person
733     ↳ auctions,
734     // client must specify win index and then we simply check if the
735     ↳ address matches for O(1) lookup vs O(n)
736     // scan. This is an option so older actions which rely on the O(n)
737     ↳ lookup because we can't change their call structure
738     // can continue to work.
739     pub user_provided_win_index: Option<Option<usize>>,
740     pub assert_bidder_signer: bool,
741     // For printing v2, the edition pda is what essentially forms a
742     ↳ backstop for bad bidders. We do not need this additional
743     // check which isn't accurate anyway when one winning config item has
744     ↳ an amount > 1.

```

```
738     pub ignore_bid_redeemed_item_check: bool,  
739 }  
740
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 29: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/state.rs:1469:1: 1473:2

```

1469 pub struct BidRedemptionTicket {
1470     // With BidRedemptionTicket is easier to hide it's legacy V1/V2 behind
1471     ↳ an internal facade,
1472     // since all of it's values are read directly off the array.
1473     pub key: Key,
1474 }
1475 metaplex/program/src/deprecated_state.rs:634:1: 637:2
1476     pub struct SafetyDepositValidationTicket {
1477     pub key: Key,
1478     pub address: Pubkey,
1479 }
1480 metaplex/program/src/state.rs:643:1: 646:2
1481     pub struct OriginalAuthorityLookup {
1482     pub key: Key,
1483     pub original_authority: Pubkey,
1484 }
1485 metaplex/program/src/state.rs:745:1: 748:2
1486     pub struct StoreConfig {
1487     pub key: Key,
1488     pub settings_uri: Option<String>,
1489 }
1490 metaplex/program/src/instruction.rs:63:1: 73:2
1491     pub struct InitAuctionManagerV2Args {
1492     pub amount_type: TupleNumericType,
1493     pub length_type: TupleNumericType,
1494     // how many ranges you can store in the AuctionWinnerTokenTypeTracker.
1495     ↳ For a limited edition single, you really
1496     // only need 1, for more complex auctions you may need more. Feel free
1497     ↳ to scale this
1498     // with the complexity of your auctions - this thing stores a range of
1499     ↳ how many unique token types

```

```
1496 // each range of people gets in the most efficient compressed way
1497 ↪ possible, but if you don't
1498 // give a high enough list length, while you may save space, you may
1499 ↪ also blow out your struct size while performing
1500 // validation and have a failed auction.
1501 pub max_ranges: u64,
1502 }
1503 metaplex/program/src/state.rs:570:1: 585:2
1504 pub struct ParticipationConfigV2 {
1505     /// Setups:
1506     /// 1. Winners get participation + not charged extra
1507     /// 2. Winners dont get participation prize
1508     pub winner_constraint: WinningConstraint,
1509
1510     /// Setups:
1511     /// 1. Losers get prize for free
1512     /// 2. Losers get prize but pay fixed price
1513     /// 3. Losers get prize but pay bid price
1514     pub non_winning_constraint: NonWinningConstraint,
1515
1516     /// Setting this field disconnects the participation prizes price from
1517     ↪ the bid. Any bid you submit, regardless
1518     /// of amount, charges you the same fixed price.
1519     pub fixed_price: Option<u64>,
1520 }
1521 metaplex/program/src/state.rs:662:1: 666:2
1522 pub struct PayoutTicket {
1523     pub key: Key,
1524     pub recipient: Pubkey,
1525     pub amount_paid: u64,
1526 }
1527 metaplex/program/src/state.rs:763:1: 767:2
1528 pub struct WhitelistedCreator {
1529     pub key: Key,
1530     pub address: Pubkey,
1531     pub activated: bool,
1532 }
1533 metaplex/program/src/deprecated_state.rs:533:1: 541:2
1534 pub struct AuctionManagerStateV1 {
1535     pub status: AuctionManagerStatus,
1536     /// When all configs are validated the auction is started and auction
1537     ↪ manager moves to Running
```

```
1534     pub winning_config_items_validated: u8,
1535
1536     pub winning_config_states: Vec<WinningConfigState>,
1537
1538     pub participation_state: Option<ParticipationStateV1>,
1539 }
1540 metaplex/program/src/deprecated_state.rs:579:1: 596:2
1541     pub struct ParticipationConfigV1 {
1542         /// Setups:
1543         /// 1. Winners get participation + not charged extra
1544         /// 2. Winners dont get participation prize
1545         pub winner_constraint: WinningConstraint,
1546
1547         /// Setups:
1548         /// 1. Losers get prize for free
1549         /// 2. Losers get prize but pay fixed price
1550         /// 3. Losers get prize but pay bid price
1551         pub non_winning_constraint: NonWinningConstraint,
1552
1553         /// The safety deposit box index in the vault containing the template
1554         ↪ for the participation prize
1555         pub safety_deposit_box_index: u8,
1556         /// Setting this field disconnects the participation prizes price from
1557         ↪ the bid. Any bid you submit, regardless
1558         /// of amount, charges you the same fixed price.
1559         pub fixed_price: Option<u64>,
1560     }
1561 metaplex/program/src/state.rs:546:1: 554:2
1562     pub struct AuctionManagerStateV2 {
1563         pub status: AuctionManagerStatus,
1564         /// When all configs are validated the auction is started and auction
1565         ↪ manager moves to Running
1566         pub safety_config_items_validated: u64,
1567         /// how many bids have been pushed to accept payment
1568         pub bids_pushed_to_accept_payment: u64,
1569
1570         pub has_participation: bool,
1571     }
1572 metaplex/program/src/state.rs:682:1: 687:2
1573     pub struct StoreIndexer {
1574         pub key: Key,
1575         pub store: Pubkey,
```

```
1573     pub page: u64,  
1574     pub auction_caches: Vec<Pubkey>,  
1575 }  
1576 metaplex/program/src/state.rs:1267:1: 1273:2  
1577     pub struct AuctionWinnerTokenTypeTracker {  
1578     pub key: Key,  
1579     pub amount_type: TupleNumericType,  
1580     pub length_type: TupleNumericType,  
1581     /// Tuple is (amount of editions or tokens given to people in this  
1582     ↪ range, length of range)  
1582     pub amount_ranges: Vec<AmountRange>,  
1583 }  
1584 metaplex/program/src/state.rs:783:1: 789:2  
1585     pub struct PrizeTrackingTicket {  
1586     pub key: Key,  
1587     pub metadata: Pubkey,  
1588     pub supply_snapshot: u64,  
1589     pub expected_redemptions: u64,  
1590     pub redemptions: u64,  
1591 }  
1592 metaplex/program/src/state.rs:726:1: 733:2  
1593     pub struct Store {  
1594     pub key: Key,  
1595     pub public: bool,  
1596     pub auction_program: Pubkey,  
1597     pub token_vault_program: Pubkey,  
1598     pub token_metadata_program: Pubkey,  
1599     pub token_program: Pubkey,  
1600 }  
1601 metaplex/program/src/state.rs:224:1: 238:2  
1602     pub struct AuctionManagerV2 {  
1603     pub key: Key,  
1604  
1605     pub store: Pubkey,  
1606  
1607     pub authority: Pubkey,  
1608  
1609     pub auction: Pubkey,  
1610  
1611     pub vault: Pubkey,  
1612  
1613     pub accept_payment: Pubkey,
```

```
1614
1615     pub state: AuctionManagerStateV2,
1616 }
1617 metaplex/program/src/state.rs:703:1: 711:2
1618     pub struct AuctionCache {
1619     pub key: Key,
1620     pub store: Pubkey,
1621     pub timestamp: i64,
1622     pub metadata: Vec<Pubkey>,
1623     pub auction: Pubkey,
1624     pub vault: Pubkey,
1625     pub auction_manager: Pubkey,
1626 }
1627 metaplex/program/src/deprecated_state.rs:57:1: 76:2
1628     pub struct AuctionManagerV1 {
1629     pub key: Key,
1630
1631     pub store: Pubkey,
1632
1633     pub authority: Pubkey,
1634
1635     pub auction: Pubkey,
1636
1637     pub vault: Pubkey,
1638
1639     pub accept_payment: Pubkey,
1640
1641     pub state: AuctionManagerStateV1,
1642
1643     pub settings: AuctionManagerSettingsV1,
1644
1645     /// True if this is only winning configs of one item each, used for
1646     ↪ optimization in saving.
1647     pub straight_shot_optimization: bool,
1648 }
1649 metaplex/program/src/state.rs:831:1: 847:2
1650     pub struct SafetyDepositConfig {
1651     pub key: Key,
1652     /// reverse lookup
1653     pub auction_manager: Pubkey,
1654     // only 255 safety deposits on vault right now but soon this will
1655     ↪ likely expand.
```



```
1654    /// safety deposit order
1655    pub order: u64,
1656    pub winning_config_type: WinningConfigType,
1657    pub amount_type: TupleNumericType,
1658    pub length_type: TupleNumericType,
1659    /// Tuple is (amount of editions or tokens given to people in this
1660    ↪ range, length of range)
1661    pub amount_ranges: Vec<AmountRange>,
1662    /// if winning config type is "Participation" then you use this to
1663    ↪ parameterize it.
1664    pub participation_config: Option<ParticipationConfigV2>,
1665    /// if winning config type is "Participation" then you use this to keep
1666    ↪ track of it.
1667    pub participation_state: Option<ParticipationStateV2>,
1668 }
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

**Issue: 30: TypeConfusion**

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/deprecated\_state.rs:624:1: 629:2

```

624 pub struct WinningConfigStateItem {
625     /// Record of primary sale or not at time of auction creation, set
626     ↳ during validation step
627     pub primary_sale_happened: bool,
628     /// Ticked to true when a prize is claimed by person who won it
629     pub claimed: bool,
630 }
631 metaplex/program/src/instruction.rs:46:1: 49:2
632     pub struct RedeemUnusedWinningConfigItemsAsAuctioneerArgs {
633         pub winning_config_item_index: u8,
634         pub proxy_call: ProxyCallAddress,
635     }
636 metaplex/program/src/deprecated_state.rs:616:1: 620:2
637     pub struct WinningConfigItem {
638         pub safety_deposit_box_index: u8,
639         pub amount: u8,
640         pub winning_config_type: WinningConfigType,
641     }

```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 31: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/deprecated\_state.rs:634:1: 637:2

```

634 pub struct SafetyDepositValidationTicket {
635     pub key: Key,
636     pub address: Pubkey,
637 }
638 metaplex/program/src/state.rs:643:1: 646:2
639     pub struct OriginalAuthorityLookup {
640         pub key: Key,
641         pub original_authority: Pubkey,
642     }
643 metaplex/program/src/state.rs:662:1: 666:2
644     pub struct PayoutTicket {
645         pub key: Key,
646         pub recipient: Pubkey,
647         pub amount_paid: u64,
648     }
649 metaplex/program/src/state.rs:763:1: 767:2
650     pub struct WhitelistedCreator {
651         pub key: Key,
652         pub address: Pubkey,
653         pub activated: bool,
654     }
655 metaplex/program/src/state.rs:682:1: 687:2
656     pub struct StoreIndexer {
657         pub key: Key,
658         pub store: Pubkey,
659         pub page: u64,
660         pub auction_caches: Vec<Pubkey>,
661     }
662 metaplex/program/src/state.rs:783:1: 789:2
663     pub struct PrizeTrackingTicket {
664         pub key: Key,
```

```
665     pub metadata: Pubkey,  
666     pub supply_snapshot: u64,  
667     pub expected_redemptions: u64,  
668     pub redemptions: u64,  
669 }  
670 metaplex/program/src/state.rs:224:1: 238:2  
671     pub struct AuctionManagerV2 {  
672     pub key: Key,  
673  
674     pub store: Pubkey,  
675  
676     pub authority: Pubkey,  
677  
678     pub auction: Pubkey,  
679  
680     pub vault: Pubkey,  
681  
682     pub accept_payment: Pubkey,  
683  
684     pub state: AuctionManagerStateV2,  
685 }  
686 metaplex/program/src/state.rs:703:1: 711:2  
687     pub struct AuctionCache {  
688     pub key: Key,  
689     pub store: Pubkey,  
690     pub timestamp: i64,  
691     pub metadata: Vec<Pubkey>,  
692     pub auction: Pubkey,  
693     pub vault: Pubkey,  
694     pub auction_manager: Pubkey,  
695 }  
696 metaplex/program/src/deprecated_state.rs:57:1: 76:2  
697     pub struct AuctionManagerV1 {  
698     pub key: Key,  
699  
700     pub store: Pubkey,  
701  
702     pub authority: Pubkey,  
703  
704     pub auction: Pubkey,  
705  
706     pub vault: Pubkey,
```

```

707
708     pub accept_payment: Pubkey,
709
710     pub state: AuctionManagerStateV1,
711
712     pub settings: AuctionManagerSettingsV1,
713
714     /// True if this is only winning configs of one item each, used for
715     ↪ optimization in saving.
716     pub straight_shot_optimization: bool,
717 }
718 metaplex/program/src/state.rs:831:1: 847:2
719     pub struct SafetyDepositConfig {
720     pub key: Key,
721     /// reverse lookup
722     pub auction_manager: Pubkey,
723     // only 255 safety deposits on vault right now but soon this will
724     ↪ likely expand.
725     /// safety deposit order
726     pub order: u64,
727     pub winning_config_type: WinningConfigType,
728     pub amount_type: TupleNumericType,
729     pub length_type: TupleNumericType,
730     /// Tuple is (amount of editions or tokens given to people in this
731     ↪ range, length of range)
732     pub amount_ranges: Vec<AmountRange>,
733     /// if winning config type is "Participation" then you use this to
734     ↪ parameterize it.
735     pub participation_config: Option<ParticipationConfigV2>,
736     /// if winning config type is "Participation" then you use this to keep
737     ↪ track of it.
738     pub participation_state: Option<ParticipationStateV2>,
739 }

```

- Call Stack

1 UnResolved

- description:
- link:

- alleviation:

## Issue: 32: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/instruction.rs:46:1: 49:2

```
46 pub struct RedeemUnusedWinningConfigItemsAsAuctioneerArgs {
47     pub winning_config_item_index: u8,
48     pub proxy_call: ProxyCallAddress,
49 }
50 metaplex/program/src/deprecated_state.rs:616:1: 620:2
51     pub struct WinningConfigItem {
52         pub safety_deposit_box_index: u8,
53         pub amount: u8,
54         pub winning_config_type: WinningConfigType,
55     }
56
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 33: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/instruction.rs:52:1: 55:2

```

52 pub struct RedeemPrintingV2BidArgs {
53     pub edition_offset: u64,
54     pub win_index: u64,
55 }
56 metaplex/program/src/instruction.rs:82:1: 85:2
57     pub struct SetStoreIndexArgs {
58         pub page: u64,
59         pub offset: u64,
60     }
61 metaplex/program/src/state.rs:805:1: 805:42
62     pub struct AmountRange(pub u64, pub u64);
63 metaplex/program/src/state.rs:849:1: 853:2
64     pub struct AmountCumulativeReturn {
65         pub amount: u64,
66         pub cumulative_amount: u64,
67         pub total_amount: u64,
68     }
69 metaplex/program/src/state.rs:101:1: 106:2
70     pub struct CommonWinningIndexChecks<'a> {
71         pub safety_deposit_info: &'a AccountInfo<'a>,
72         pub winning_index: usize,
73         pub auction_manager_v1_ignore_claim: bool,
74         pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
75     }
76 metaplex/program/src/state.rs:108:1: 116:2
77     pub struct PrintingV2CalculationChecks<'a> {
78         pub safety_deposit_info: &'a AccountInfo<'a>,
79         pub winning_index: usize,
80         pub auction_manager_v1_ignore_claim: bool,
81         pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
82         pub short_circuit_total: bool,

```



```
83     pub edition_offset: u64,  
84     pub winners: usize,  
85 }  
86 metaplex/program/src/processor/redeem_participation_bid.rs:29:1: 39:2  
87     struct V2Accounts<'a> {  
88         pub prize_tracking_ticket_info: &'a AccountInfo<'a>,  
89         pub new_metadata_account_info: &'a AccountInfo<'a>,  
90         pub new_edition_account_info: &'a AccountInfo<'a>,  
91         pub master_edition_account_info: &'a AccountInfo<'a>,  
92         pub mint_info: &'a AccountInfo<'a>,  
93         pub edition_marker_info: &'a AccountInfo<'a>,  
94         pub mint_authority_info: &'a AccountInfo<'a>,  
95         pub metadata_account_info: &'a AccountInfo<'a>,  
96         pub auction_extended_info: &'a AccountInfo<'a>,  
97     }  
98 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:185:1:  
99 ↪ 203:2  
100     pub struct SupplyLogicCheckArgs<'a, 'b> {  
101         pub program_id: &'a Pubkey,  
102         pub auction_manager_info: &'a AccountInfo<'a>,  
103         pub metadata_info: &'a AccountInfo<'a>,  
104         pub edition_info: &'a AccountInfo<'a>,  
105         pub metadata_authority_info: &'a AccountInfo<'a>,  
106         pub original_authority_lookup_info: &'a AccountInfo<'a>,  
107         pub rent_info: &'a AccountInfo<'a>,  
108         pub system_info: &'a AccountInfo<'a>,  
109         pub payer_info: &'a AccountInfo<'a>,  
110         pub token_metadata_program_info: &'a AccountInfo<'a>,  
111         pub safety_deposit_token_store_info: &'a AccountInfo<'a>,  
112         pub auction_manager: &'b dyn AuctionManager,  
113         pub winning_config_type: &'b WinningConfigType,  
114         pub metadata: &'b Metadata,  
115         pub safety_deposit: &'b SafetyDepositBox,  
116         pub store: &'b Store,  
117         pub total_amount_requested: u64,  
118     }  
119 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:69:1: 89:2  
120     pub struct CommonCheckArgs<'a, 'b> {  
121         pub program_id: &'a Pubkey,  
122         pub auction_manager_info: &'a AccountInfo<'a>,  
123         pub metadata_info: &'a AccountInfo<'a>,  
124         pub original_authority_lookup_info: &'a AccountInfo<'a>,  
125     }
```

```
124     pub whitelisted_creator_info: &'a AccountInfo<'a>,
125     pub safety_deposit_info: &'a AccountInfo<'a>,
126     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
127     pub edition_info: &'a AccountInfo<'a>,
128     pub vault_info: &'a AccountInfo<'a>,
129     pub mint_info: &'a AccountInfo<'a>,
130     pub token_metadata_program_info: &'a AccountInfo<'a>,
131     pub auction_manager_store_info: &'a AccountInfo<'a>,
132     pub authority_info: &'a AccountInfo<'a>,
133     pub store: &'b Store,
134     pub auction_manager: &'b dyn AuctionManager,
135     pub metadata: &'b Metadata,
136     pub safety_deposit: &'b SafetyDepositBox,
137     pub vault: &'b Vault,
138     pub winning_config_type: &'b WinningConfigType,
139 }
140 metaplex/program/src/utils.rs:389:1: 420:2
141     pub struct CommonRedeemCheckArgs<'a> {
142     pub program_id: &'a Pubkey,
143     pub auction_manager_info: &'a AccountInfo<'a>,
144     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
145     pub destination_info: &'a AccountInfo<'a>,
146     pub bid_redemption_info: &'a AccountInfo<'a>,
147     pub safety_deposit_info: &'a AccountInfo<'a>,
148     pub vault_info: &'a AccountInfo<'a>,
149     pub auction_info: &'a AccountInfo<'a>,
150     pub auction_extended_info: Option<&'a AccountInfo<'a>>,
151     pub bidder_metadata_info: &'a AccountInfo<'a>,
152     pub bidder_info: &'a AccountInfo<'a>,
153     pub token_program_info: &'a AccountInfo<'a>,
154     pub token_vault_program_info: &'a AccountInfo<'a>,
155     pub token_metadata_program_info: &'a AccountInfo<'a>,
156     pub store_info: &'a AccountInfo<'a>,
157     pub rent_info: &'a AccountInfo<'a>,
158     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
159     pub is_participation: bool,
160     // If this is being called by the auctioneer to pull prizes out they
161     ↳ overwrite the win index
162     // they would normally get if they themselves bid for whatever win
163     ↳ index they choose.
164     pub overwrite_win_index: Option<usize>,
165     // In newer endpoints, to conserve CPU and make way for 10,000 person
166     ↳ auctions,
```

```
164 // client must specify win index and then we simply check if the
    ↳ address matches for O(1) lookup vs O(n)
165 // scan. This is an option so older actions which rely on the O(n)
    ↳ lookup because we can't change their call structure
166 // can continue to work.
167 pub user_provided_win_index: Option<Option<usize>>,
168 pub assert_bidder_signer: bool,
169 // For printing v2, the edition pda is what essentially forms a
    ↳ backstop for bad bidders. We do not need this additional
170 // check which isn't accurate anyway when one winning config item has
    ↳ an amount > 1.
171 pub ignore_bid_redeemed_item_check: bool,
172 }
173
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 34: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/instruction.rs:82:1: 85:2

```

82 pub struct SetStoreIndexArgs {
83     pub page: u64,
84     pub offset: u64,
85 }
86 metaplex/program/src/state.rs:805:1: 805:42
87     pub struct AmountRange(pub u64, pub u64);
88 metaplex/program/src/state.rs:849:1: 853:2
89     pub struct AmountCumulativeReturn {
90         pub amount: u64,
91         pub cumulative_amount: u64,
92         pub total_amount: u64,
93     }
94 metaplex/program/src/state.rs:101:1: 106:2
95     pub struct CommonWinningIndexChecks<'a> {
96         pub safety_deposit_info: &'a AccountInfo<'a>,
97         pub winning_index: usize,
98         pub auction_manager_v1_ignore_claim: bool,
99         pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
100     }
101 metaplex/program/src/state.rs:108:1: 116:2
102     pub struct PrintingV2CalculationChecks<'a> {
103         pub safety_deposit_info: &'a AccountInfo<'a>,
104         pub winning_index: usize,
105         pub auction_manager_v1_ignore_claim: bool,
106         pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
107         pub short_circuit_total: bool,
108         pub edition_offset: u64,
109         pub winners: usize,
110     }
111 metaplex/program/src/processor/redeem_participation_bid.rs:29:1: 39:2
112     struct V2Accounts<'a> {

```

```
113     pub prize_tracking_ticket_info: &'a AccountInfo<'a>,
114     pub new_metadata_account_info: &'a AccountInfo<'a>,
115     pub new_edition_account_info: &'a AccountInfo<'a>,
116     pub master_edition_account_info: &'a AccountInfo<'a>,
117     pub mint_info: &'a AccountInfo<'a>,
118     pub edition_marker_info: &'a AccountInfo<'a>,
119     pub mint_authority_info: &'a AccountInfo<'a>,
120     pub metadata_account_info: &'a AccountInfo<'a>,
121     pub auction_extended_info: &'a AccountInfo<'a>,
122 }
123 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:185:1:
124 ↪ 203:2
125     pub struct SupplyLogicCheckArgs<'a, 'b> {
126     pub program_id: &'a Pubkey,
127     pub auction_manager_info: &'a AccountInfo<'a>,
128     pub metadata_info: &'a AccountInfo<'a>,
129     pub edition_info: &'a AccountInfo<'a>,
130     pub metadata_authority_info: &'a AccountInfo<'a>,
131     pub original_authority_lookup_info: &'a AccountInfo<'a>,
132     pub rent_info: &'a AccountInfo<'a>,
133     pub system_info: &'a AccountInfo<'a>,
134     pub payer_info: &'a AccountInfo<'a>,
135     pub token_metadata_program_info: &'a AccountInfo<'a>,
136     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
137     pub auction_manager: &'b dyn AuctionManager,
138     pub winning_config_type: &'b WinningConfigType,
139     pub metadata: &'b Metadata,
140     pub safety_deposit: &'b SafetyDepositBox,
141     pub store: &'b Store,
142     pub total_amount_requested: u64,
143 }
144 metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:69:1: 89:2
145     pub struct CommonCheckArgs<'a, 'b> {
146     pub program_id: &'a Pubkey,
147     pub auction_manager_info: &'a AccountInfo<'a>,
148     pub metadata_info: &'a AccountInfo<'a>,
149     pub original_authority_lookup_info: &'a AccountInfo<'a>,
150     pub whitelisted_creator_info: &'a AccountInfo<'a>,
151     pub safety_deposit_info: &'a AccountInfo<'a>,
152     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
153     pub edition_info: &'a AccountInfo<'a>,
154     pub vault_info: &'a AccountInfo<'a>
```

```

154     pub mint_info: &'a AccountInfo<'a>,
155     pub token_metadata_program_info: &'a AccountInfo<'a>,
156     pub auction_manager_store_info: &'a AccountInfo<'a>,
157     pub authority_info: &'a AccountInfo<'a>,
158     pub store: &'b Store,
159     pub auction_manager: &'b dyn AuctionManager,
160     pub metadata: &'b Metadata,
161     pub safety_deposit: &'b SafetyDepositBox,
162     pub vault: &'b Vault,
163     pub winning_config_type: &'b WinningConfigType,
164 }
165 metaplex/program/src/utils.rs:389:1: 420:2
166     pub struct CommonRedeemCheckArgs<'a> {
167     pub program_id: &'a Pubkey,
168     pub auction_manager_info: &'a AccountInfo<'a>,
169     pub safety_deposit_token_store_info: &'a AccountInfo<'a>,
170     pub destination_info: &'a AccountInfo<'a>,
171     pub bid_redemption_info: &'a AccountInfo<'a>,
172     pub safety_deposit_info: &'a AccountInfo<'a>,
173     pub vault_info: &'a AccountInfo<'a>,
174     pub auction_info: &'a AccountInfo<'a>,
175     pub auction_extended_info: Option<&'a AccountInfo<'a>>,
176     pub bidder_metadata_info: &'a AccountInfo<'a>,
177     pub bidder_info: &'a AccountInfo<'a>,
178     pub token_program_info: &'a AccountInfo<'a>,
179     pub token_vault_program_info: &'a AccountInfo<'a>,
180     pub token_metadata_program_info: &'a AccountInfo<'a>,
181     pub store_info: &'a AccountInfo<'a>,
182     pub rent_info: &'a AccountInfo<'a>,
183     pub safety_deposit_config_info: Option<&'a AccountInfo<'a>>,
184     pub is_participation: bool,
185     // If this is being called by the auctioneer to pull prizes out they
186     ↳ overwrite the win index
187     // they would normally get if they themselves bid for whatever win
188     ↳ index they choose.
189     pub overwrite_win_index: Option<usize>,
190     // In newer endpoints, to conserve CPU and make way for 10,000 person
191     ↳ auctions,
192     // client must specify win index and then we simply check if the
193     ↳ address matches for O(1) lookup vs O(n)
194     // scan. This is an option so older actions which rely on the O(n)
195     ↳ lookup because we can't change their call structure

```

```
191 // can continue to work.
192 pub user_provided_win_index: Option<Option<usize>>,
193 pub assert_bidder_signer: bool,
194 // For printing v2, the edition pda is what essentially forms a
195 ↪ backstop for bad bidders. We do not need this additional
196 // check which isn't accurate anyway when one winning config item has
197 ↪ an amount > 1.
198 pub ignore_bid_redeemed_item_check: bool,
199 }
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Issue: 35: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/state.rs:643:1: 646:2

```
643 pub struct OriginalAuthorityLookup {
644     pub key: Key,
645     pub original_authority: Pubkey,
646 }
647 metaplex/program/src/state.rs:662:1: 666:2
648     pub struct PayoutTicket {
649         pub key: Key,
650         pub recipient: Pubkey,
651         pub amount_paid: u64,
652     }
653 metaplex/program/src/state.rs:763:1: 767:2
654     pub struct WhitelistedCreator {
655         pub key: Key,
656         pub address: Pubkey,
657         pub activated: bool,
658     }
659 metaplex/program/src/state.rs:682:1: 687:2
660     pub struct StoreIndexer {
661         pub key: Key,
662         pub store: Pubkey,
663         pub page: u64,
664         pub auction_caches: Vec<Pubkey>,
665     }
666 metaplex/program/src/state.rs:783:1: 789:2
667     pub struct PrizeTrackingTicket {
668         pub key: Key,
669         pub metadata: Pubkey,
670         pub supply_snapshot: u64,
671         pub expected_redemptions: u64,
672         pub redemptions: u64,
673     }
```



```
674 metaplex/program/src/state.rs:224:1: 238:2
675     pub struct AuctionManagerV2 {
676     pub key: Key,
677
678     pub store: Pubkey,
679
680     pub authority: Pubkey,
681
682     pub auction: Pubkey,
683
684     pub vault: Pubkey,
685
686     pub accept_payment: Pubkey,
687
688     pub state: AuctionManagerStateV2,
689 }
690 metaplex/program/src/state.rs:703:1: 711:2
691     pub struct AuctionCache {
692     pub key: Key,
693     pub store: Pubkey,
694     pub timestamp: i64,
695     pub metadata: Vec<Pubkey>,
696     pub auction: Pubkey,
697     pub vault: Pubkey,
698     pub auction_manager: Pubkey,
699 }
700 metaplex/program/src/deprecated_state.rs:57:1: 76:2
701     pub struct AuctionManagerV1 {
702     pub key: Key,
703
704     pub store: Pubkey,
705
706     pub authority: Pubkey,
707
708     pub auction: Pubkey,
709
710     pub vault: Pubkey,
711
712     pub accept_payment: Pubkey,
713
714     pub state: AuctionManagerStateV1,
715
```

```

716     pub settings: AuctionManagerSettingsV1,
717
718     /// True if this is only winning configs of one item each, used for
719     ↳ optimization in saving.
720     pub straight_shot_optimization: bool,
721 }
722 metaplex/program/src/state.rs:831:1: 847:2
723     pub struct SafetyDepositConfig {
724     pub key: Key,
725     /// reverse lookup
726     pub auction_manager: Pubkey,
727     // only 255 safety deposits on vault right now but soon this will
728     ↳ likely expand.
729     /// safety deposit order
730     pub order: u64,
731     pub winning_config_type: WinningConfigType,
732     pub amount_type: TupleNumericType,
733     pub length_type: TupleNumericType,
734     /// Tuple is (amount of editions or tokens given to people in this
735     ↳ range, length of range)
736     pub amount_ranges: Vec<AmountRange>,
737     /// if winning config type is "Participation" then you use this to
738     ↳ parameterize it.
739     pub participation_config: Option<ParticipationConfigV2>,
740     /// if winning config type is "Participation" then you use this to keep
741     ↳ track of it.
742     pub participation_state: Option<ParticipationStateV2>,
743 }

```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

**Issue: 36: TypeConfusion**

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

metaplex/program/src/state.rs:662:1: 666:2

```

662 pub struct PayoutTicket {
663     pub key: Key,
664     pub recipient: Pubkey,
665     pub amount_paid: u64,
666 }
667 metaplex/program/src/state.rs:682:1: 687:2
668     pub struct StoreIndexer {
669         pub key: Key,
670         pub store: Pubkey,
671         pub page: u64,
672         pub auction_caches: Vec<Pubkey>,
673     }
674 metaplex/program/src/state.rs:783:1: 789:2
675     pub struct PrizeTrackingTicket {
676         pub key: Key,
677         pub metadata: Pubkey,
678         pub supply_snapshot: u64,
679         pub expected_redemptions: u64,
680         pub redemptions: u64,
681     }
682 metaplex/program/src/state.rs:703:1: 711:2
683     pub struct AuctionCache {
684         pub key: Key,
685         pub store: Pubkey,
686         pub timestamp: i64,
687         pub metadata: Vec<Pubkey>,
688         pub auction: Pubkey,
689         pub vault: Pubkey,
690         pub auction_manager: Pubkey,
691     }
692 metaplex/program/src/state.rs:831:1: 847:2

```

```
693 pub struct SafetyDepositConfig {
694     pub key: Key,
695     /// reverse lookup
696     pub auction_manager: Pubkey,
697     // only 255 safety deposits on vault right now but soon this will
698     ↳ likely expand.
699     /// safety deposit order
700     pub order: u64,
701     pub winning_config_type: WinningConfigType,
702     pub amount_type: TupleNumericType,
703     pub length_type: TupleNumericType,
704     /// Tuple is (amount of editions or tokens given to people in this
705     ↳ range, length of range)
706     pub amount_ranges: Vec<AmountRange>,
707     /// if winning config type is "Participation" then you use this to
708     ↳ parameterize it.
709     pub participation_config: Option<ParticipationConfigV2>,
710     /// if winning config type is "Participation" then you use this to keep
711     ↳ track of it.
712     pub participation_state: Option<ParticipationStateV2>,
713 }
```

- Call Stack

1 UnResolved

- description:
- link:
- alleviation:

## Appendix

Copied from <https://leaderboard.certik.io/projects/aave>

### Finding Categories

#### Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

#### Mathematical Operations

Mathematical Operation findings relate to mishandling of math formulas, such as overflows, incorrect operations etc.

#### Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.

#### Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of `private` or `delete`.

#### Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

#### Checksum Calculation Method

The “Checksum” field in the “Audit Scope” section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux “sha256sum” command against the target file.

## Disclaimer

Copied from <https://leaderboard.certik.io/projects/aave>

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.