VRust

Security Assessment

O2Lab VRust Team

18/02/2022 21:28:18

Contents

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	https://github.com/parasol-aser/vrust
sha256	Unknown

Audit Summary

Delivery Date	18/02/2022
Audit Methodology	Static Analysis
Key Components	

Vulnerability Summary

Vulnerability Level	Total
Critical	219
Major	0
Medium	0
Minor	0
Informational	0
Discussion	0

Findings

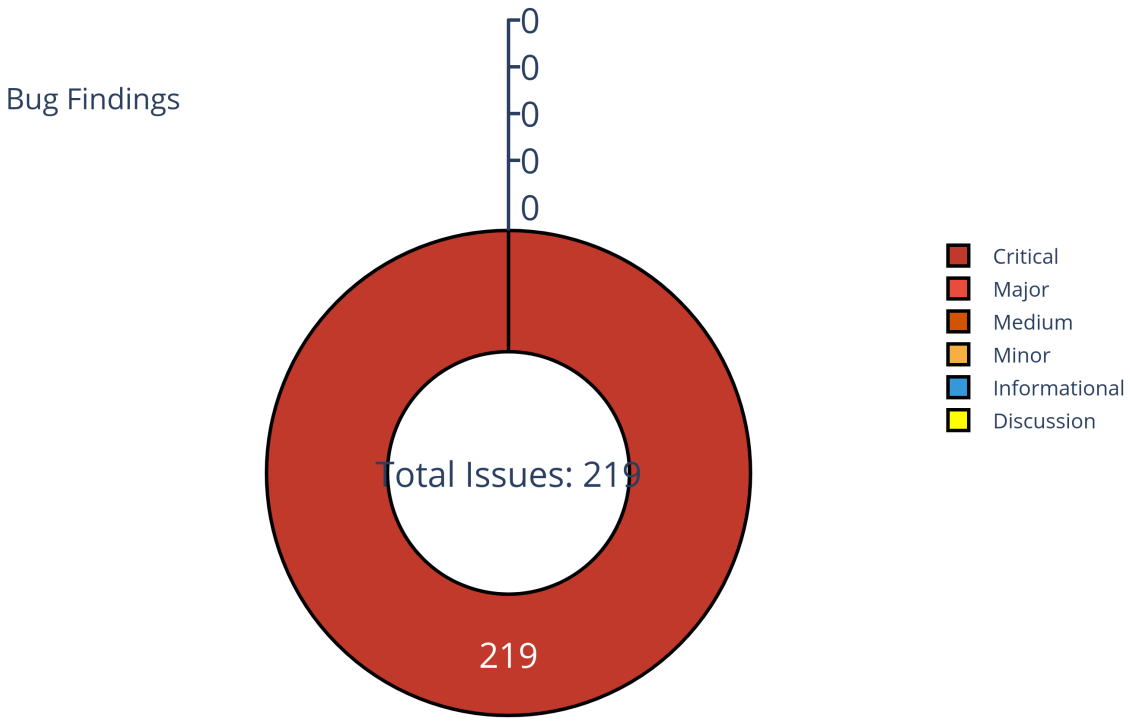

Figure 1: Findings

ID	Title	Category	Severity	Status
INT_CVE_0	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_1	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_2	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_3	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_4	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_5	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_6	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_7	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_8	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_9	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_10	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_11	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_12	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_13	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_14	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_15	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_16	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_17	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_18	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_19	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_20	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_21	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_22	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_23	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_24	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_25	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_26	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_27	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_28	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_29	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_30	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_31	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_32	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_33	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_34	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_35	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_36	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_37	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_38	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_39	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_40	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_41	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_42	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_43	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_44	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_45	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_46	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_47	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_48	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_49	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_50	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_51	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_52	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_53	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_54	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_55	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_56	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_57	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_58	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_59	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_60	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_61	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_62	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_63	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_64	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_65	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_66	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_67	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_68	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_69	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_70	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_71	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_72	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_73	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_74	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_75	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_76	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_77	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_78	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_79	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_80	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_81	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_82	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_83	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_84	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_85	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_86	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_87	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_88	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_89	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_90	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_91	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_92	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_93	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_94	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_95	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_96	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_97	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_98	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_99	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_100	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_101	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_102	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_103	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_104	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_105	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_106	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_107	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_108	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_109	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_110	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_111	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_112	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_113	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_114	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_115	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_116	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_117	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_118	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_119	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_120	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_121	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_122	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_123	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_124	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_125	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_126	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_127	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_128	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_129	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_130	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_131	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_132	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_133	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_134	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_135	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_136	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_137	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_138	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_139	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_140	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_141	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_142	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_143	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_144	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_145	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_146	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_147	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_148	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_149	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_150	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_151	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_152	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_153	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_154	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_155	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_156	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_157	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_158	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_159	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_160	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_161	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_162	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_163	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_164	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
INT_CVE_165	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_166	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_167	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_168	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_169	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_170	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_171	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_172	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_173	Overflow	Integer Overflow wpa	Critical	UnResolved
TYP_CVE_0	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_1	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_2	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_3	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_4	Instruction id not checked error	Instruction id issue	Critical	UnResolved

ID	Title	Category	Severity	Status
TYP_CVE_5	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_6	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_7	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_8	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_9	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_10	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_11	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_12	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_13	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_14	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_15	Instruction id not checked error	Instruction id issue	Critical	UnResolved

ID	Title	Category	Severity	Status
TYP_CVE_16	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_17	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_18	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_19	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_20	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_21	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_22	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_23	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_24	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_25	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_26	Instruction id not checked error	Instruction id issue	Critical	UnResolved

ID	Title	Category	Severity	Status
TYP_CVE_27	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_28	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_29	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_30	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_31	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_32	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_33	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_34	Instruction id not checked error	Instruction id issue	Critical	UnResolved
CHK_CVE_0	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_1	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_2	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_3	is_owner	Missing Owner Check	Critical	UnResolved

ID	Title	Category	Severity	Status
CHK_CVE_4	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_5	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_6	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_7	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_8	is_owner	Missing Owner Check	Critical	UnResolved
CHK_CVE_9	is_owner	Missing Owner Check	Critical	UnResolved

Issue: INT_CVE_0: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
```

```
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_1: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::rent::Rent::minimum_balance(){//
                                 ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                 ↪  1ecc6299db9ec823/solana-program-
                                 ↪  1.9.5/src/rent.rs:55:5: 59:6
                                 ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_2: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                     fn solana_program::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_3: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_4: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_auction_cache::process_set_auction_cache(){//
           ↪  metaplex/program/src/processor/set_auction_cache.rs:19:1: 143:2
           ↪  }
4             fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                 fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_5: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_auction_cache::process_set_auction_cache(){//
           ↪  metaplex/program/src/processor/set_auction_cache.rs:19:1: 143:2
           ↪  }
4              fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                      fn solana_program::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_6: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_index::process_set_store_index(){//
           ↪  metaplex/program/src/processor/set_store_index.rs:22:1: 217:2 }
4             fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                     fn solana_program::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_7: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_index::process_set_store_index(){//
           ↪  metaplex/program/src/processor/set_store_index.rs:22:1: 217:2 }
4              fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_8: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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
                ↪ Err(MetaplexError::ExpectedAboveAuctionCacheToBeProvided.into());
165         }
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 ==
            ↪ indexer.auction_caches.len() - 1 {
172             &above_cache
173         } else {
174
```

- 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_index::process_set_store_index(){//
          ↪ metaplex/program/src/processor/set_store_index.rs:22:1: 217:2 }
4
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_9: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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(){//
                ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                       fn state::BidRedemptionTicket::check_ticket(){//
                        ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_10: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_11: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_12: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 }
```

```
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 }
    fn utils::create_or_allocate_account_raw(){//
    ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
        fn
        ↪  solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-
        ↪  1.9.5/src/rent.rs:55:5: 59:6
        ↪  }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_13: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                           fn
                            ↪  solana_program::rent::Rent::minimum_balance(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:55:5: 59:6
                            ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_14: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_15: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_16: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_17: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_18: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_finish(){//
                ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_19: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1303:13: 1303:43

```
1303 offset += amount_type as usize
1304
```

- Code Context

Vulnerability at Line: 1303

```
1298         let mut offset: usize = 7;
1299         let mut amount_ranges = vec![];
1300         for _ in 0..length_of_array {
1301             let amount = get_number_from_data(data, amount_type, offset);
1302
1303             offset += amount_type as usize;
1304
1305             let length = get_number_from_data(data, length_type, offset);
1306
1307             amount_ranges.push(AmountRange(amount, length));
1308
```

- 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::from_account_info(){//
              ↪  metaplex/program/src/state.rs:1280:5: 1317:6 }
```

```
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_20: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/arrayref-0.3.6/src/lib.rs:65:40:65:46

```
65 offset
66
```

- Code Context

– Function Definition:

```
862 fn get_number_from_data(data: &Ref<&mut [u8]>, data_type: TupleNumericType,
    ↪  offset: usize) -> u64
863
```

Vulnerability at Line: 862

```
862 fn get_number_from_data(data: &Ref<&mut [u8]>, data_type: TupleNumericType,
    ↪  offset: usize) -> u64 {
863     return match data_type {
864         TupleNumericType::U8 => data[offset] as u64,
865         TupleNumericType::U16 => u16::from_le_bytes(*array_ref![data,
            ↪  offset, 2]) as u64,
866         TupleNumericType::U32 => u32::from_le_bytes(*array_ref![data,
            ↪  offset, 4]) as u64,
867
```

Other Use Case for Variable: offset

```
864         TupleNumericType::U8 => data[offset] as u64,
```

```
865         TupleNumericType::U16 => u16::from_le_bytes(*array_ref![data,
            ↪  offset, 2]) as u64,
```

```
866         TupleNumericType::U32 => u32::from_le_bytes(*array_ref![data,
            ↪  offset, 4]) as u64,
```

```
867         TupleNumericType::U64 => u64::from_le_bytes(*array_ref![data,
            ↪  offset, 8]),
```

- 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::from_account_info(){//
               ↪  metaplex/program/src/state.rs:1280:5: 1317:6 }
5                  fn state::get_number_from_data(){//
                   ↪  metaplex/program/src/state.rs:862:1: 870:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_21: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/arrayref-0.3.6/src/lib.rs:65:40:65:46

```
65 offset
66
```

- Code Context

– Function Definition:

```
862 fn get_number_from_data(data: &Ref<&mut [u8]>, data_type: TupleNumericType,
    ↪  offset: usize) -> u64
863
```

Vulnerability at Line: 862

```
862 fn get_number_from_data(data: &Ref<&mut [u8]>, data_type: TupleNumericType,
    ↪  offset: usize) -> u64 {
863     return match data_type {
864         TupleNumericType::U8 => data[offset] as u64,
865         TupleNumericType::U16 => u16::from_le_bytes(*array_ref![data,
            ↪  offset, 2]) as u64,
866         TupleNumericType::U32 => u32::from_le_bytes(*array_ref![data,
            ↪  offset, 4]) as u64,
867
```

Other Use Case for Variable: offset

```
864         TupleNumericType::U8 => data[offset] as u64,
```

```
865         TupleNumericType::U16 => u16::from_le_bytes(*array_ref![data,
            ↪  offset, 2]) as u64,
```

```
866         TupleNumericType::U32 => u32::from_le_bytes(*array_ref![data,
            ↪  offset, 4]) as u64,
```

```
867         TupleNumericType::U64 => u64::from_le_bytes(*array_ref![data,
            ↪  offset, 8]),
```

- 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::from_account_info(){//
               ↪  metaplex/program/src/state.rs:1280:5: 1317:6 }
5                  fn state::get_number_from_data(){//
                   ↪  metaplex/program/src/state.rs:862:1: 870:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_22: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/arrayref-0.3.6/src/lib.rs:65:40:65:46

```
65 offset
66
```

- Code Context

– Function Definition:

```
862 fn get_number_from_data(data: &Ref<&mut [u8]>, data_type: TupleNumericType,
    ↪  offset: usize) -> u64
863
```

Vulnerability at Line: 862

```
862 fn get_number_from_data(data: &Ref<&mut [u8]>, data_type: TupleNumericType,
    ↪  offset: usize) -> u64 {
863     return match data_type {
864         TupleNumericType::U8 => data[offset] as u64,
865         TupleNumericType::U16 => u16::from_le_bytes(*array_ref![data,
            ↪  offset, 2]) as u64,
866         TupleNumericType::U32 => u32::from_le_bytes(*array_ref![data,
            ↪  offset, 4]) as u64,
867
```

Other Use Case for Variable: offset

```
864         TupleNumericType::U8 => data[offset] as u64,
```

```
865         TupleNumericType::U16 => u16::from_le_bytes(*array_ref![data,
            ↪  offset, 2]) as u64,
```

```
866         TupleNumericType::U32 => u32::from_le_bytes(*array_ref![data,
            ↪  offset, 4]) as u64,
```

```
867         TupleNumericType::U64 => u64::from_le_bytes(*array_ref![data,
            ↪  offset, 8]),
```

- 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::from_account_info(){//
               ↪  metaplex/program/src/state.rs:1280:5: 1317:6 }
5                  fn state::get_number_from_data(){//
                   ↪  metaplex/program/src/state.rs:862:1: 870:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_23: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1308:13: 1308:43

```
1308 offset += length_type as usize
1309
```

- Code Context

Vulnerability at Line: 1308

```
1303             offset += amount_type as usize;
1304
1305             let length = get_number_from_data(data, length_type, offset);
1306
1307             amount_ranges.push(AmountRange(amount, length));
1308             offset += length_type as usize;
1309         }
1310
1311         Ok(AuctionWinnerTokenTypeTracker {
1312             key: Key::AuctionWinnerTokenTypeTrackerV1,
1313
```

- 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::from_account_info(){//
               ↪  metaplex/program/src/state.rs:1280:5: 1317:6 }
```

```
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_24: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_supply_logic_check(){//
               ↪  meta-
               ↪  plex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1:
               ↪  381:2 }
```

```
5                    fn utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_25: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_supply_logic_check(){//
               ↪  meta-
               ↪  plex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1:
               ↪  381:2 }
```

```
fn utils::create_or_allocate_account_raw(){//
↪  metaplex/program/src/utils.rs:212:1: 257:2 }
    fn solana_program::rent::Rent::minimum_balance(){//
    ↪  /home/ubuntu/.cargo/registry/src/github.com-
    ↪  1ecc6299db9ec823/solana-program-
    ↪  1.9.5/src/rent.rs:55:5: 59:6
    ↪  }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_26: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_supply_logic_check(){//
               ↪  meta-
               ↪  plex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1:
               ↪  381:2 }
```

```
5                    fn utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_27: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_28: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_29: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_30: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_31: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1462:13: 1462:48

```
1462 offset += self.length_type as usize
1463
```

- Code Context

Vulnerability at Line: 1462

```
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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_32: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_33: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:906:15: 906:97

```
906 (self.amount_type as usize + self.length_type as usize) *
    ↪  self.amount_ranges.len()
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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_34: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:905:16: 906:97

```
905 BASE_SAFETY_CONFIG_SIZE
906             + (self.amount_type as usize + self.length_type as usize) *
    ↪  self.amount_ranges.len()
907
```

- Code Context

Vulnerability at Line: 905

```
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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_35: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 }
```

```
fn utils::create_or_allocate_account_raw(){//
↪  metaplex/program/src/utils.rs:212:1: 257:2 }
    fn solana_program::rent::Rent::minimum_balance(){//
    ↪  /home/ubuntu/.cargo/registry/src/github.com-
    ↪  1ecc6299db9ec823/solana-program-
    ↪  1.9.5/src/rent.rs:55:5: 59:6
    ↪  }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_36: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_37: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_38: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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(){//
                        ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_39: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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 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(){//
                   ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }
6                      fn state::write_length_type(){//
                       ↪  metaplex/program/src/state.rs:887:1: 900:2 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_40: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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 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(){//
                   ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }
6                      fn state::write_length_type(){//
                       ↪  metaplex/program/src/state.rs:887:1: 900:2 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_41: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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 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(){//
                   ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }
6                      fn state::write_length_type(){//
                       ↪  metaplex/program/src/state.rs:887:1: 900:2 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_42: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1184:13: 1184:48

```
1184 offset += self.length_type as usize
1185
```

- Code Context

Vulnerability at Line: 1184

```
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         match &self.participation_config {
1188             Some(val) => {
1189
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_43: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1190:22: 1190:32

```
1190 offset + 1
1191
```

- Code Context

Vulnerability at Line: 1190

```
1185         }
1186
1187         match &self.participation_config {
1188             Some(val) => {
1189                 data[offset] = 1;
1190                 data[offset + 1] = val.winner_constraint as u8;
1191                 data[offset + 2] = val.non_winning_constraint as u8;
1192                 offset += 3;
1193                 match val.fixed_price {
1194                     Some(val) => {
1195
```

Other Use Case for Variable: offset + 1

```
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
```

```
1214                 *array_mut_ref![data, offset + 1, 8] =
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  metaplex/program/src/entrypoint.rs:14:1: 25:2 }
    fn processor::process_instruction(){//
    ↪  metaplex/program/src/processor.rs:50:1: 169:2 }
        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 }
            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 }
                fn state::SafetyDepositConfig::create(){//
                ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_44: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1191:22: 1191:32

```
1191 offset + 2
1192
```

- Code Context

Vulnerability at Line: 1191

```
1186
1187         match &self.participation_config {
1188             Some(val) => {
1189                 data[offset] = 1;
1190                 data[offset + 1] = val.winner_constraint as u8;
1191                 data[offset + 2] = val.non_winning_constraint as u8;
1192                 offset += 3;
1193                 match val.fixed_price {
1194                     Some(val) => {
1195                         data[offset] = 1;
1196
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_45: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1192:17: 1192:28

```
1192 offset += 3
1193
```

- Code Context

Vulnerability at Line: 1192

```
1187         match &self.participation_config {
1188             Some(val) => {
1189                 data[offset] = 1;
1190                 data[offset + 1] = val.winner_constraint as u8;
1191                 data[offset + 2] = val.non_winning_constraint as u8;
1192                 offset += 3;
1193                 match val.fixed_price {
1194                     Some(val) => {
1195                         data[offset] = 1;
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
1197
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_46: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1196:47: 1196:57

```
1196 offset + 1
1197
```

- Code Context

Vulnerability at Line: 1190

```
1185         }
1186
1187         match &self.participation_config {
1188             Some(val) => {
1189                 data[offset] = 1;
1190                 data[offset + 1] = val.winner_constraint as u8;
1191                 data[offset + 2] = val.non_winning_constraint as u8;
1192                 offset += 3;
1193                 match val.fixed_price {
1194                     Some(val) => {
1195
```

Other Use Case for Variable: offset + 1

```
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
```

```
1214                 *array_mut_ref![data, offset + 1, 8] =
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  metaplex/program/src/entrypoint.rs:14:1: 25:2 }
    fn processor::process_instruction(){//
    ↪  metaplex/program/src/processor.rs:50:1: 169:2 }
        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 }
            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 }
                fn state::SafetyDepositConfig::create(){//
                ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_47: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

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

```
290 offset
291
```

- Code Context

Vulnerability at Line: 1179

```
1174         data[WINNING_CONFIG_POSITION] = self.winning_config_type as u8;
1175         data[AMOUNT_POSITION] = self.amount_type as u8;
1176         data[LENGTH_POSITION] = self.length_type as u8;
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
```

Other Use Case for Variable: offset

```
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;
```

```
1189                data[offset] = 1;
```

```
1190                data[offset + 1] = val.winner_constraint as u8;
```

```
1191                data[offset + 2] = val.non_winning_constraint as u8;
```

```
1192                offset += 3;
```

```
1195                        data[offset] = 1;
```

```
1196                        *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
```

```
1197                        offset += 9;
```

```
1200                        data[offset] = 0;
```

```
1201                        offset += 1;
```

```
1206                data[offset] = 0;
```

```
1207                offset += 1;
```

```
1213                data[offset] = 1;
```

```
1214                *array_mut_ref![data, offset + 1, 8] =
```

```
1219                data[offset] = 0;
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  metaplex/program/src/entrypoint.rs:14:1: 25:2 }
    fn processor::process_instruction(){//
    ↪  metaplex/program/src/processor.rs:50:1: 169:2 }
        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 }
            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 }
                fn state::SafetyDepositConfig::create(){//
                ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_48: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1197:25: 1197:36

```
1197 offset += 9
1198
```

- Code Context

Vulnerability at Line: 1197

```
1192                 offset += 3;
1193                 match val.fixed_price {
1194                     Some(val) => {
1195                         data[offset] = 1;
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
1197                         offset += 9;
1198                     }
1199                     None => {
1200                         data[offset] = 0;
1201                         offset += 1;
1202
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_49: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1201:25: 1201:36

```
1201 offset += 1
1202
```

- Code Context

Vulnerability at Line: 1201

```
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
1197                         offset += 9;
1198                     }
1199                     None => {
1200                         data[offset] = 0;
1201                         offset += 1;
1202                     }
1203                 }
1204             }
1205             None => {
1206
```

Other Use Case for Variable: offset += 1

```
1207                 offset += 1;
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_50: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1207:17: 1207:28

```
1207 offset += 1
1208
```

- Code Context

Vulnerability at Line: 1201

```
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
1197                         offset += 9;
1198                     }
1199                     None => {
1200                         data[offset] = 0;
1201                         offset += 1;
1202                     }
1203                 }
1204             }
1205             None => {
1206
```

Other Use Case for Variable: offset += 1

```
1207                 offset += 1;
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_51: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1214:39: 1214:49

```
1214 offset + 1
1215
```

- Code Context

Vulnerability at Line: 1190

```
1185         }
1186
1187         match &self.participation_config {
1188             Some(val) => {
1189                 data[offset] = 1;
1190                 data[offset + 1] = val.winner_constraint as u8;
1191                 data[offset + 2] = val.non_winning_constraint as u8;
1192                 offset += 3;
1193                 match val.fixed_price {
1194                     Some(val) => {
1195
```

Other Use Case for Variable: offset + 1

```
1196                         *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();
```

```
1214                 *array_mut_ref![data, offset + 1, 8] =
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  metaplex/program/src/entrypoint.rs:14:1: 25:2 }
    fn processor::process_instruction(){//
    ↪  metaplex/program/src/processor.rs:50:1: 169:2 }
        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 }
            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 }
                fn state::SafetyDepositConfig::create(){//
                ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_52: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

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

```
290 offset
291
```

- Code Context

Vulnerability at Line: 1179

```
1174         data[WINNING_CONFIG_POSITION] = self.winning_config_type as u8;
1175         data[AMOUNT_POSITION] = self.amount_type as u8;
1176         data[LENGTH_POSITION] = self.length_type as u8;
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
```

Other Use Case for Variable: offset

```
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;

1189                data[offset] = 1;

1190                data[offset + 1] = val.winner_constraint as u8;

1191                data[offset + 2] = val.non_winning_constraint as u8;

1192                offset += 3;

1195                        data[offset] = 1;

1196                        *array_mut_ref![data, offset + 1, 8] =
↪  val.to_le_bytes();

1197                        offset += 9;

1200                        data[offset] = 0;

1201                        offset += 1;

1206                data[offset] = 0;

1207                offset += 1;

1213                data[offset] = 1;

1214                *array_mut_ref![data, offset + 1, 8] =

1219                data[offset] = 0;
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  metaplex/program/src/entrypoint.rs:14:1: 25:2 }
    fn processor::process_instruction(){//
    ↪  metaplex/program/src/processor.rs:50:1: 169:2 }
        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 }
            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 }
                fn state::SafetyDepositConfig::create(){//
                ↪  metaplex/program/src/state.rs:1164:5: 1227:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_53: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_54: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_55: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                   fn solana_program::rent::Rent::minimum_balance(){//
                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                    ↪  1ecc6299db9ec823/solana-program-
                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                    ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_56: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_57: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1277:16: 1278:92

```
1277 BASE_TRACKER_SIZE
1278             + (self.amount_type as usize + self.length_type as usize) *
     ↪  range_size as usize
1279
```

- Code Context

Vulnerability at Line: 1277

```
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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_58: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                 fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_59: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_60: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                   fn solana_program::rent::Rent::minimum_balance(){//
                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                    ↪  1ecc6299db9ec823/solana-program-
                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                    ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_61: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

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

```
290 offset
291
```

- Code Context

– Function Definition:

```
872 fn write_amount_type(
873     data: &mut RefMut<&mut [u8]>,
874     amount_type: TupleNumericType,
875     offset: usize,
876     range: &AmountRange,
877 )
878
```

Vulnerability at Line: 875

```
872 fn write_amount_type(
873     data: &mut RefMut<&mut [u8]>,
874     amount_type: TupleNumericType,
875     offset: usize,
876     range: &AmountRange,
877 ) {
878     match amount_type {
879         TupleNumericType::U8 => data[offset] = range.0 as u8,
880
```

Other Use Case for Variable: offset

```
879         TupleNumericType::U8 => data[offset] = range.0 as u8,
```

```
880         TupleNumericType::U16 => *array_mut_ref![data, offset, 2] =
            ↪  (range.0 as u16).to_le_bytes(),
```

```
881         TupleNumericType::U32 => *array_mut_ref![data, offset, 4] =
            ↪  (range.0 as u32).to_le_bytes(),
```

```
882         TupleNumericType::U64 => *array_mut_ref![data, offset, 8] =
            ↪  range.0.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::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::save(){//
               ↪  metaplex/program/src/state.rs:1451:5: 1464:6 }
5                  fn state::write_amount_type(){//
                   ↪  metaplex/program/src/state.rs:872:1: 885:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_62: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

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

```
290 offset
291
```

- Code Context

– Function Definition:

```
872 fn write_amount_type(
873     data: &mut RefMut<&mut [u8]>,
874     amount_type: TupleNumericType,
875     offset: usize,
876     range: &AmountRange,
877 )
878
```

Vulnerability at Line: 875

```
872 fn write_amount_type(
873     data: &mut RefMut<&mut [u8]>,
874     amount_type: TupleNumericType,
875     offset: usize,
876     range: &AmountRange,
877 ) {
878     match amount_type {
879         TupleNumericType::U8 => data[offset] = range.0 as u8,
880
```

Other Use Case for Variable: offset

```
879         TupleNumericType::U8 => data[offset] = range.0 as u8,
```

```
880         TupleNumericType::U16 => *array_mut_ref![data, offset, 2] =
            ↪  (range.0 as u16).to_le_bytes(),
```

```
881         TupleNumericType::U32 => *array_mut_ref![data, offset, 4] =
            ↪  (range.0 as u32).to_le_bytes(),
```

```
882         TupleNumericType::U64 => *array_mut_ref![data, offset, 8] =
            ↪  range.0.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::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::save(){//
               ↪  metaplex/program/src/state.rs:1451:5: 1464:6 }
5                  fn state::write_amount_type(){//
                   ↪  metaplex/program/src/state.rs:872:1: 885:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_63: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

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

```
290 offset
291
```

- Code Context

– Function Definition:

```
872 fn write_amount_type(
873     data: &mut RefMut<&mut [u8]>,
874     amount_type: TupleNumericType,
875     offset: usize,
876     range: &AmountRange,
877 )
878
```

Vulnerability at Line: 875

```
872 fn write_amount_type(
873     data: &mut RefMut<&mut [u8]>,
874     amount_type: TupleNumericType,
875     offset: usize,
876     range: &AmountRange,
877 ) {
878     match amount_type {
879         TupleNumericType::U8 => data[offset] = range.0 as u8,
880
```

Other Use Case for Variable: offset

```
879         TupleNumericType::U8 => data[offset] = range.0 as u8,
```

```
880         TupleNumericType::U16 => *array_mut_ref![data, offset, 2] =
            ↪  (range.0 as u16).to_le_bytes(),
```

```
881         TupleNumericType::U32 => *array_mut_ref![data, offset, 4] =
            ↪  (range.0 as u32).to_le_bytes(),
```

```
882         TupleNumericType::U64 => *array_mut_ref![data, offset, 8] =
            ↪  range.0.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::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::save(){//
               ↪  metaplex/program/src/state.rs:1451:5: 1464:6 }
5                  fn state::write_amount_type(){//
                   ↪  metaplex/program/src/state.rs:872:1: 885:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_64: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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::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::save(){//
               ↪  metaplex/program/src/state.rs:1451:5: 1464:6 }
```

```
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_65: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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::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::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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_66: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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::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::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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_67: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.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::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::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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_68: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

metaplex/program/src/state.rs:1462:13: 1462:48

```
1462 offset += self.length_type as usize
1463
```

- Code Context

Vulnerability at Line: 1462

```
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::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::save(){//
              ↪  metaplex/program/src/state.rs:1451:5: 1464:6 }
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_69: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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(){//
                ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                       fn state::BidRedemptionTicket::check_ticket(){//
                        ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_70: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_71: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_72: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_73: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 }
```

```
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 }
    fn utils::create_or_allocate_account_raw(){//
    ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
        fn
        ↪  solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-
        ↪  1.9.5/src/rent.rs:55:5: 59:6
        ↪  }
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_74: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 }
```

```
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 }
    fn utils::create_or_allocate_account_raw(){//
    ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
        fn
        ↪  solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-
        ↪  1.9.5/src/rent.rs:55:5: 59:6
        ↪  }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_75: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                           fn
                            ↪  solana_program::rent::Rent::minimum_balance(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:55:5: 59:6
                            ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_76: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_77: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_78: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_79: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                 fn solana_program::rent::Rent::minimum_balance(){//
                                  ↪ /home/ubuntu/.cargo/registry/src/github.com-
                                  ↪ 1ecc6299db9ec823/solana-program-
                                  ↪ 1.9.5/src/rent.rs:55:5: 59:6
                                  ↪ }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_80: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_finish(){//
                ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_81: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::withdraw_master_edition::process_withdraw_master_edition(){//
           ↪  metaplex/program/src/processor/withdraw_master_edition.rs:20:1:
           ↪  181:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_82: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::withdraw_master_edition::process_withdraw_master_edition(){//
           ↪  metaplex/program/src/processor/withdraw_master_edition.rs:20:1:
           ↪  181:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_83: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::withdraw_master_edition::process_withdraw_master_edition(){//
           ↪  metaplex/program/src/processor/withdraw_master_edition.rs:20:1:
           ↪  181:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_84: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::withdraw_master_edition::process_withdraw_master_edition(){//
           ↪  metaplex/program/src/processor/withdraw_master_edition.rs:20:1:
           ↪  181:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_85: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::withdraw_master_edition::process_withdraw_master_edition(){//
           ↪  metaplex/program/src/processor/withdraw_master_edition.rs:20:1:
           ↪  181:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                fn solana_program::rent::Rent::minimum_balance(){//
                                 ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                 ↪  1ecc6299db9ec823/solana-program-
                                 ↪  1.9.5/src/rent.rs:55:5: 59:6
                                 ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_86: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::withdraw_master_edition::process_withdraw_master_edition(){//
           ↪  metaplex/program/src/processor/withdraw_master_edition.rs:20:1:
           ↪  181:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_87: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4             fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
```

```
5                    fn state::BidRedemptionTicket::check_ticket(){//
                     ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
6                    fn
                     ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                     ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_88: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4              fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                  fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
6                      fn solana_program::rent::Rent::is_exempt(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:62:5: 64:6
                       ↪  }
```

```
7                                   fn
                                    ↪  solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_89: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4              fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                  fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
6                      fn solana_program::rent::Rent::is_exempt(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:62:5: 64:6
                       ↪  }
```

```
7                                   fn
                                    ↪  solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_90: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4              fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                  fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_91: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4             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 }
5                 fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_92: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4             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 }
5                 fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_93: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4              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 }
```

```
5                    fn utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_94: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_printing_v2_bid::process_redeem_printing_v2_bid(){//
          ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
          ↪  350:2 }
4             fn utils::common_redeem_finish(){//
              ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_95: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                 fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_96: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4              fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                  fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_97: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4              fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                  fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_98: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_printing_v2_bid::process_redeem_printing_v2_bid(){//
          ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
          ↪  350:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
```

```
5                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                       fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_99: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
```

```
4           fn proces-
            ↪ sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
            ↪ meta-
            ↪ plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
            ↪ 167:2 }
5               fn utils::common_redeem_checks(){//
                ↪ metaplex/program/src/utils.rs:509:1: 681:2 }
6                   fn state::BidRedemptionTicket::check_ticket(){//
                    ↪ metaplex/program/src/state.rs:1476:5: 1520:6 }
7                       fn
                        ↪ state::BidRedemptionTicket::get_index_and_mask(){//
                        ↪ metaplex/program/src/state.rs:1522:5:
                        ↪ 1544:6 }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_100: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
```

```
5                   fn utils::common_redeem_checks(){//
                    ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
6                       fn utils::assert_rent_exempt(){//
                        ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
7                           fn solana_program::rent::Rent::is_exempt(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:62:5: 64:6
                            ↪  }
8       fn solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6
        ↪  }
9
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_101: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
```

```
5                   fn utils::common_redeem_checks(){//
                    ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
6                       fn utils::assert_rent_exempt(){//
                        ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
7                           fn solana_program::rent::Rent::is_exempt(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:62:5: 64:6
                            ↪  }
8       fn solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6
        ↪  }
9
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_102: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4              fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
```

```
5                   fn utils::common_redeem_checks(){//
                    ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
6                       fn utils::assert_rent_exempt(){//
                        ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
7                           fn solana_program::rent::Rent::is_exempt(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:62:5: 64:6
                            ↪  }
8       fn solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6
        ↪  }
9
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_103: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_unused_winning_config_items_as_auctioneer::process_redeem_unused
          ↪  meta-
          ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
          ↪  32:2 }
4             fn proces-
              ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
              ↪  meta-
              ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
              ↪  167:2 }
```

```
5                       fn utils::common_redeem_finish(){//
                        ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_104: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
```

```
fn utils::common_redeem_finish(){// metaplex/program/src/utils.rs:702:1: 776:2 }
    fn utils::create_or_allocate_account_raw(){// metaplex/program/src/utils.rs:212:1: 257:2 }
        fn solana_program::rent::Rent::minimum_balance(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_105: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
```

```
fn utils::common_redeem_finish(){//
↪  metaplex/program/src/utils.rs:702:1: 776:2 }
    fn utils::create_or_allocate_account_raw(){//
    ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
        fn
        ↪  solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-
        ↪  1.9.5/src/rent.rs:55:5: 59:6
        ↪  }
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_106: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4              fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
```

```
fn utils::common_redeem_finish(){// metaplex/program/src/utils.rs:702:1: 776:2 }
    fn utils::create_or_allocate_account_raw(){// metaplex/program/src/utils.rs:212:1: 257:2 }
        fn solana_program::rent::Rent::minimum_balance(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6 }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_107: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
```

```
4               fn proces-
                ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
                ↪  meta-
                ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
                ↪  167:2 }
5                   fn utils::common_redeem_finish(){//
                    ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
7                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5:
                            ↪  1544:6 }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_108: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
```

```
4               fn processor::redeem_bid::process_redeem_bid(){//
                ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                   fn utils::common_redeem_checks(){//
                    ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
6                       fn state::BidRedemptionTicket::check_ticket(){//
                        ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
7                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5:
                            ↪  1544:6 }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_109: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                 fn utils::common_redeem_checks(){//
                   ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
```

```
6                         fn utils::assert_rent_exempt(){//
                           ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
7                             fn solana_program::rent::Rent::is_exempt(){//
                               ↪  /home/ubuntu/.cargo/registry/src/github.com-
                               ↪  1ecc6299db9ec823/solana-program-
                               ↪  1.9.5/src/rent.rs:62:5: 64:6
                               ↪  }
8         fn solana_program::rent::Rent::minimum_balance(){//
          ↪  /home/ubuntu/.cargo/registry/src/github.com-
          ↪  1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6
          ↪  }
9
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_110: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4              fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                  fn utils::common_redeem_checks(){//
                   ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
```

```
6                         fn utils::assert_rent_exempt(){//
                           ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
7                             fn solana_program::rent::Rent::is_exempt(){//
                               ↪  /home/ubuntu/.cargo/registry/src/github.com-
                               ↪  1ecc6299db9ec823/solana-program-
                               ↪  1.9.5/src/rent.rs:62:5: 64:6
                               ↪  }
8         fn solana_program::rent::Rent::minimum_balance(){//
          ↪  /home/ubuntu/.cargo/registry/src/github.com-
          ↪  1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6
          ↪  }
9
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_111: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4              fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                  fn utils::common_redeem_checks(){//
                   ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
```

```
6                         fn utils::assert_rent_exempt(){//
                           ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
7                             fn solana_program::rent::Rent::is_exempt(){//
                               ↪  /home/ubuntu/.cargo/registry/src/github.com-
                               ↪  1ecc6299db9ec823/solana-program-
                               ↪  1.9.5/src/rent.rs:62:5: 64:6
                               ↪  }
8         fn solana_program::rent::Rent::minimum_balance(){//
          ↪  /home/ubuntu/.cargo/registry/src/github.com-
          ↪  1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:55:5: 59:6
          ↪  }
9
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_112: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_unused_winning_config_items_as_auctioneer::process_redeem_unused
          ↪  meta-
          ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
          ↪  32:2 }
4             fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
```

```
5                       fn utils::common_redeem_finish(){//
                        ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_113: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                 fn utils::common_redeem_finish(){//
                   ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
```

```
6                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                          fn
                           ↪  solana_program::rent::Rent::minimum_balance(){//
                           ↪  /home/ubuntu/.cargo/registry/src/github.com-
                           ↪  1ecc6299db9ec823/solana-program-
                           ↪  1.9.5/src/rent.rs:55:5: 59:6
                           ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_114: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4              fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                  fn utils::common_redeem_finish(){//
                   ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
```

```
6                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                          fn
                           ↪  solana_program::rent::Rent::minimum_balance(){//
                           ↪  /home/ubuntu/.cargo/registry/src/github.com-
                           ↪  1ecc6299db9ec823/solana-program-
                           ↪  1.9.5/src/rent.rs:55:5: 59:6
                           ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_115: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4              fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                  fn utils::common_redeem_finish(){//
                   ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
```

```
6                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                          fn
                           ↪  solana_program::rent::Rent::minimum_balance(){//
                           ↪  /home/ubuntu/.cargo/registry/src/github.com-
                           ↪  1ecc6299db9ec823/solana-program-
                           ↪  1.9.5/src/rent.rs:55:5: 59:6
                           ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_116: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
```

```
4           fn processor::redeem_bid::process_redeem_bid(){//
            ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5               fn utils::common_redeem_finish(){//
                ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6                   fn state::BidRedemptionTicket::save(){//
                    ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
7                       fn
                        ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                        ↪  metaplex/program/src/state.rs:1522:5:
                        ↪  1544:6 }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_117: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_participation::process_deprecated_validate_particip
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_participation.rs:24:1:
           ↪  176:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_118: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_participation::process_deprecated_validate_particip
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_participation.rs:24:1:
           ↪  176:2 }
4             fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                 fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_119: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_participation::process_deprecated_validate_particip
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_participation.rs:24:1:
           ↪  176:2 }
4              fn utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_120: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::set_whitelisted_creator::process_set_whitelisted_creator(){//
           ↪  metaplex/program/src/processor/set_whitelisted_creator.rs:16:1:
           ↪  84:2 }
4              fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_121: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::set_whitelisted_creator::process_set_whitelisted_creator(){//
           ↪  metaplex/program/src/processor/set_whitelisted_creator.rs:16:1:
           ↪  84:2 }
4              fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_122: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9:58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::set_whitelisted_creator::process_set_whitelisted_creator(){//
           ↪  metaplex/program/src/processor/set_whitelisted_creator.rs:16:1:
           ↪  84:2 }
4             fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                   fn solana_program::rent::Rent::minimum_balance(){//
                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                    ↪  1ecc6299db9ec823/solana-program-
                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                    ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_123: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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(){//
           ↪  metaplex/program/src/processor/set_store.rs:90:1: 120:2 }
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::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
```

```
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_124: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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(){//
           ↪  metaplex/program/src/processor/set_store.rs:90:1: 120:2 }
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::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
```

```
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_125: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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(){//
           ↪  metaplex/program/src/processor/set_store.rs:90:1: 120:2 }
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::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_126: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                 fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_127: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_128: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::assert_rent_exempt(){//
               ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
5                  fn solana_program::rent::Rent::is_exempt(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:62:5: 64:6
                   ↪  }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_129: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_130: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
5                  fn solana_program::rent::Rent::minimum_balance(){//
                   ↪  /home/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/rent.rs:55:5: 59:6
                   ↪  }
```

```
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_131: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                   fn solana_program::rent::Rent::minimum_balance(){//
                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                    ↪  1ecc6299db9ec823/solana-program-
                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                    ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_132: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/VRust/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 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                       fn mpl_auction::processor::BidState::amount(){//
                        ↪  /home/ubuntu/VRust/metaplex-program-
                        ↪  library/auction/program/src/processor.rs:646:5:
                        ↪  657:6 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_133: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:650:33: 650:55

```
650 bids.len() - index - 1
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 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                       fn mpl_auction::processor::BidState::amount(){//
                        ↪  /home/ubuntu/VRust/metaplex-program-
                        ↪  library/auction/program/src/processor.rs:646:5:
                        ↪  657:6 }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_134: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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
                    ↪  artists get their cut
126                 (10000 - metadata.data.seller_fee_basis_points) as u128
127             } else {
128                 // during primary sale, auctioneer (creator index not
                    ↪  provided)
```

```
                // get none of the proceeds
                0u128

```

- Call Stack

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

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_135: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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(){//
                ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                       fn state::BidRedemptionTicket::check_ticket(){//
                        ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_136: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_137: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_138: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_139: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 }
```

```
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 }
    fn utils::create_or_allocate_account_raw(){//
    ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
        fn
        ↪  solana_program::rent::Rent::minimum_balance(){//
        ↪  /home/ubuntu/.cargo/registry/src/github.com-
        ↪  1ecc6299db9ec823/solana-program-
        ↪  1.9.5/src/rent.rs:55:5: 59:6
        ↪  }

```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_140: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                           fn
                            ↪  solana_program::rent::Rent::minimum_balance(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:55:5: 59:6
                            ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_141: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
7                           fn
                            ↪  solana_program::rent::Rent::minimum_balance(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:55:5: 59:6
                            ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_142: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_143: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_144: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_145: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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 utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_146: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_finish(){//
                ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_147: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
```

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

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_148: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
4             fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                 fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_149: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
4             fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                 fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_150: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
4              fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                  fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
```

```
6                       fn solana_program::rent::Rent::is_exempt(){//
                        ↪ /home/ubuntu/.cargo/registry/src/github.com-
                        ↪ 1ecc6299db9ec823/solana-program-
                        ↪ 1.9.5/src/rent.rs:62:5: 64:6
                        ↪ }
7                       fn
                            ↪ solana_program::rent::Rent::minimum_balance(){//
                            ↪ /home/ubuntu/.cargo/registry/src/github.com-
                            ↪ 1ecc6299db9ec823/solana-program-
                            ↪ 1.9.5/src/rent.rs:55:5: 59:6
                            ↪ }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_151: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
          ↪  meta-
          ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
          ↪  167:2 }
4             fn utils::common_redeem_finish(){//
              ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
```

```
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_152: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                 fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_153: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
4              fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                  fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                 fn solana_program::rent::Rent::minimum_balance(){//
                                  ↪ /home/ubuntu/.cargo/registry/src/github.com-
                                  ↪ 1ecc6299db9ec823/solana-program-
                                  ↪ 1.9.5/src/rent.rs:55:5: 59:6
                                  ↪ }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_154: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
4              fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                  fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                fn solana_program::rent::Rent::minimum_balance(){//
                                 ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                 ↪  1ecc6299db9ec823/solana-program-
                                 ↪  1.9.5/src/rent.rs:55:5: 59:6
                                 ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_155: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
           ↪  meta-
           ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
           ↪  167:2 }
```

```
4               fn utils::common_redeem_finish(){//
                ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                           fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_156: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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 processor::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
```

```
5                       fn state::BidRedemptionTicket::check_ticket(){//
                        ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
6                       fn
                        ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                        ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_157: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4              fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                  fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
6                      fn solana_program::rent::Rent::is_exempt(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:62:5: 64:6
                       ↪  }
```

```
7                                   fn
                                    ↪  solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_158: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
5                 fn utils::assert_rent_exempt(){//
                   ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
6                     fn solana_program::rent::Rent::is_exempt(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:62:5: 64:6
                       ↪  }
```

```
7                                   fn
                                    ↪  solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_159: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9:58:40

```
(((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
            * self.exemption_threshold)

```

- Code Context

Vulnerability at Line: 57

```
pub fn minimum_balance(&self, data_len: usize) -> u64 {
        let bytes = data_len as u64;
        (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
↪   as f64
            * self.exemption_threshold) as u64
    }

```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  metaplex/program/src/entrypoint.rs:14:1: 25:2 }
    fn processor::process_instruction(){//
    ↪  metaplex/program/src/processor.rs:50:1: 169:2 }
        fn processor::redeem_bid::process_redeem_bid(){//
        ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
            fn utils::common_redeem_checks(){//
            ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
                fn utils::assert_rent_exempt(){//
                ↪  metaplex/program/src/utils.rs:59:1: 65:2 }
                    fn solana_program::rent::Rent::is_exempt(){//
                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                    ↪  1ecc6299db9ec823/solana-program-
                    ↪  1.9.5/src/rent.rs:62:5: 64:6
                    ↪  }
```

```
7                                   fn
                                    ↪  solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
8
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_160: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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 processor::redeem_bid::process_redeem_bid(){//
          ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_finish(){//
              ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_161: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4              fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                  fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                      fn solana_program::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
```

```
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_162: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                 fn utils::create_or_allocate_account_raw(){//
                   ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                     fn solana_program::rent::Rent::minimum_balance(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/rent.rs:55:5: 59:6
                       ↪  }
```

```
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_163: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                     fn utils::create_or_allocate_account_raw(){//
                       ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
6                                   fn solana_program::rent::Rent::minimum_balance(){//
                                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                                    ↪  1ecc6299db9ec823/solana-program-
                                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                                    ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_164: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	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 processor::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
```

```
5                       fn state::BidRedemptionTicket::save(){//
                        ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                       fn
                            ↪  state::BidRedemptionTicket::get_index_and_mask(){//
                            ↪  metaplex/program/src/state.rs:1522:5: 1544:6 }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_165: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1
           ↪  237:2 }
4             fn proces-
               ↪  sor::validate_safety_deposit_box_v2::assert_supply_logic_check(){//
               ↪  meta-
               ↪  plex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1:
               ↪  381:2 }
```

```
5                    fn utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_166: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_
          ↪  meta-
          ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1
          ↪  237:2 }
4             fn proces-
               ↪  sor::validate_safety_deposit_box_v2::assert_supply_logic_check(){//
               ↪  meta-
               ↪  plex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1:
               ↪  381:2 }
```

```
5                    fn utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_167: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1
           ↪  237:2 }
4              fn proces-
               ↪  sor::validate_safety_deposit_box_v2::assert_supply_logic_check(){//
               ↪  meta-
               ↪  plex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1:
               ↪  381:2 }
```

```
5                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                           fn solana_program::rent::Rent::minimum_balance(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:55:5: 59:6
                            ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_168: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11:57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1
           ↪  237:2 }
4             fn proces-
               ↪  sor::deprecated_validate_safety_deposit_box_v1::make_safety_deposit_vali
               ↪  meta-
               ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:
               ↪  65:2 }
```

```
5                    fn utils::create_or_allocate_account_raw(){//
                     ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                        fn solana_program::rent::Rent::minimum_balance(){//
                         ↪  /home/ubuntu/.cargo/registry/src/github.com-
                         ↪  1ecc6299db9ec823/solana-program-
                         ↪  1.9.5/src/rent.rs:55:5: 59:6
                         ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_169: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10:57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1
           ↪  237:2 }
4             fn proces-
               ↪  sor::deprecated_validate_safety_deposit_box_v1::make_safety_deposit_vali
               ↪  meta-
               ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:
               ↪  65:2 }
```

```
5                   fn utils::create_or_allocate_account_raw(){//
                    ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                       fn solana_program::rent::Rent::minimum_balance(){//
                        ↪  /home/ubuntu/.cargo/registry/src/github.com-
                        ↪  1ecc6299db9ec823/solana-program-
                        ↪  1.9.5/src/rent.rs:55:5: 59:6
                        ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_170: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9: 58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1
           ↪  237:2 }
4              fn proces-
               ↪  sor::deprecated_validate_safety_deposit_box_v1::make_safety_deposit_vali
               ↪  meta-
               ↪  plex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:
               ↪  65:2 }
```

```
5                       fn utils::create_or_allocate_account_raw(){//
                        ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
6                           fn solana_program::rent::Rent::minimum_balance(){//
                            ↪  /home/ubuntu/.cargo/registry/src/github.com-
                            ↪  1ecc6299db9ec823/solana-program-
                            ↪  1.9.5/src/rent.rs:55:5: 59:6
                            ↪  }
7
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_171: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:11: 57:45

```
57 (ACCOUNT_STORAGE_OVERHEAD + bytes)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_init_auction_manager_v1::process_deprecated_init_auction_man
          ↪  meta-
          ↪  plex/program/src/processor/deprecated_init_auction_manager_v1.rs:20:1:
          ↪  133:2 }
4             fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                   fn solana_program::rent::Rent::minimum_balance(){//
                    ↪  /home/ubuntu/.cargo/registry/src/github.com-
                    ↪  1ecc6299db9ec823/solana-program-
                    ↪  1.9.5/src/rent.rs:55:5: 59:6
                    ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_172: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:10: 57:76

```
57 ((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
58
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_init_auction_manager_v1::process_deprecated_init_auction_man
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_init_auction_manager_v1.rs:20:1:
           ↪  133:2 }
4              fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                       fn solana_program::rent::Rent::minimum_balance(){//
                        ↪  /home/ubuntu/.cargo/registry/src/github.com-
                        ↪  1ecc6299db9ec823/solana-program-
                        ↪  1.9.5/src/rent.rs:55:5: 59:6
                        ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_173: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/rent.rs:57:9:58:40

```
57 (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58             * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55 pub fn minimum_balance(&self, data_len: usize) -> u64 {
56         let bytes = data_len as u64;
57         (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
   ↪  as f64
58             * self.exemption_threshold) as u64
59     }
60
```

- 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::deprecated_init_auction_manager_v1::process_deprecated_init_auction_man
           ↪  meta-
           ↪  plex/program/src/processor/deprecated_init_auction_manager_v1.rs:20:1:
           ↪  133:2 }
4              fn utils::create_or_allocate_account_raw(){//
               ↪  metaplex/program/src/utils.rs:212:1: 257:2 }
```

```
5                    fn solana_program::rent::Rent::minimum_balance(){//
                     ↪  /home/ubuntu/.cargo/registry/src/github.com-
                     ↪  1ecc6299db9ec823/solana-program-
                     ↪  1.9.5/src/rent.rs:55:5: 59:6
                     ↪  }
6
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: TYP_CVE_0: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account_info.rs:81:5: 83:6

```
81 pub fn data_is_empty(&self) -> bool {
82         self.data.borrow().is_empty()
83     }
84
```

- 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
                      ↪  solana_program::account_info::AccountInfo::<'a>::data_is_empty()
                      ↪  /home/ubuntu/.cargo/registry/src/github.com-
                      ↪  1ecc6299db9ec823/solana-program-
                      ↪  1.9.5/src/account_info.rs:81:5: 83:6
                      ↪  }
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_1: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/processor/set_store.rs:19:1: 88:2

```
pub fn set_store_logic<'a>(
    public: bool,
    program_id: &Pubkey,
    auction_program_info: &'a AccountInfo<'a>,
    token_vault_program_info: &'a AccountInfo<'a>,
    rent_info: &'a AccountInfo<'a>,
    system_info: &'a AccountInfo<'a>,
    token_metadata_program_info: &'a AccountInfo<'a>,
    token_program_info: &'a AccountInfo<'a>,
    store_info: &'a AccountInfo<'a>,
    admin_wallet_info: &'a AccountInfo<'a>,
    payer_info: &'a AccountInfo<'a>,
) -> ProgramResult {
    assert_signer(payer_info)?;
    assert_signer(admin_wallet_info)?;
    if !store_info.data_is_empty() {
        assert_owned_by(store_info, program_id)?;
    }

    let store_bump = assert_derivation(
        program_id,
        store_info,
        &[
            PREFIX.as_bytes(),
            program_id.as_ref(),
            admin_wallet_info.key.as_ref(),
        ],
    )?;

    if store_info.data_is_empty() {
        create_or_allocate_account_raw(
```

```
            *program_id,
            store_info,
            rent_info,
            system_info,
            payer_info,
            MAX_STORE_SIZE,
            &[
                PREFIX.as_bytes(),
                program_id.as_ref(),
                admin_wallet_info.key.as_ref(),
                &[store_bump],
            ],
        )?;
    }

    let mut store = Store::from_account_info(store_info)?;
    store.key = Key::StoreV1;
    store.public = public;
    // Keys can only be set once, once set from all 0s, they are immutable.
    if store.token_program == solana_program::system_program::id() {
        store.token_program = *token_program_info.key;
    }

    if store.token_program != spl_token::id() {
        return Err(MetaplexError::InvalidTokenProgram.into());
    }

    if store.token_vault_program == solana_program::system_program::id() {
        store.token_vault_program = *token_vault_program_info.key;
    }
    if store.token_metadata_program == solana_program::system_program::id()
    ↪ {
        store.token_metadata_program = *token_metadata_program_info.key;
    }
    if store.auction_program == solana_program::system_program::id() {
        store.auction_program = *auction_program_info.key;
    }
    store.serialize(&mut *store_info.data.borrow_mut())?;
    Ok(())
}

```

- Call Stack

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

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_2: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account_info.rs:81:5: 83:6

```
81 pub fn data_is_empty(&self) -> bool {
82         self.data.borrow().is_empty()
83     }
84
```

- 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
              ↪  solana_program::account_info::AccountInfo::<'a>::data_is_empty(){//
              ↪  /home/ubuntu/.cargo/registry/src/github.com-
              ↪  1ecc6299db9ec823/solana-program-
              ↪  1.9.5/src/account_info.rs:81:5: 83:6
              ↪  }
5
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_3: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account_info.rs:73:5: 75:6

```
73 pub fn data_len(&self) -> usize {
74         self.data.borrow().len()
75     }
76
```

- 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_auction_cache::process_set_auction_cache(){//
           ↪  metaplex/program/src/processor/set_auction_cache.rs:19:1: 143:2
           ↪  }
4              fn mpl_auction::processor::AuctionData::from_account_info(){//
               ↪  /home/ubuntu/VRust/metaplex-program-
               ↪  library/auction/program/src/processor.rs:316:5: 324:6
               ↪  }
5                      fn
                       ↪  solana_program::account_info::AccountInfo::<'a>::data_len(){//
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/account_info.rs:73:5: 75:6
                       ↪  }
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_4: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:212:1: 221:2

```
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         10 => return
            ↪  Ok(Box::new(AuctionManagerV2::from_account_info(account)?)),
219         _ => return Err(MetaplexError::DataTypeMismatch.into()),
220     };
221 }
222 
```

- 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:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_5: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/utils.rs:509:1: 681:2

```
509 pub fn common_redeem_checks(
510     args: CommonRedeemCheckArgs,
511 ) -> Result<CommonRedeemReturn, ProgramError> {
512     let CommonRedeemCheckArgs {
513         program_id,
514         auction_manager_info,
515         safety_deposit_token_store_info,
516         destination_info,
517         bid_redemption_info,
518         safety_deposit_info,
519         vault_info,
520         auction_info,
521         auction_extended_info,
522         bidder_metadata_info,
523         bidder_info,
524         token_program_info,
525         token_vault_program_info,
526         token_metadata_program_info,
527         rent_info,
528         store_info,
529         safety_deposit_config_info,
530         is_participation,
531         overwrite_win_index,
532         user_provided_win_index,
533         assert_bidder_signer,
534         ignore_bid_redeemed_item_check,
535     } = args;
536
537     let rent = &Rent::from_account_info(&rent_info)?;
538
539     let mut auction_manager: Box<dyn AuctionManager> =
     ↪  get_auction_manager(auction_manager_info)?;
```

```
540     let store_data = store_info.data.borrow();
541     let cancelled: bool;
542 
543     let auction_program = Pubkey::new_from_array(*array_ref![store_data, 2,
        ↪  32]);
544     let token_vault_program =
        ↪  Pubkey::new_from_array(*array_ref![store_data, 34, 32]);
545     let token_metadata_program =
        ↪  Pubkey::new_from_array(*array_ref![store_data, 66, 32]);
546     let token_program = Pubkey::new_from_array(*array_ref![store_data, 98,
        ↪  32]);
547 
548     let mut redemption_bump_seed: u8 = 0;
549     if overwrite_win_index.is_some() {
550         cancelled = false;
551 
552         if *bidder_info.key != auction_manager.authority() {
553             return Err(MetaplexError::MustBeAuctioneer.into());
554         }
555     } else {
556         let bidder_metadata_data = bidder_metadata_info.data.borrow();
557         if bidder_metadata_data[80] == 0 {
558             cancelled = false
559         } else {
560             cancelled = true;
561         }
562         assert_owned_by(bidder_metadata_info, &auction_program)?;
563         assert_derivation(
564             &auction_program,
565             bidder_metadata_info,
566             &[
567                 mpl_auction::PREFIX.as_bytes(),
568                 auction_program.as_ref(),
569                 auction_info.key.as_ref(),
570                 bidder_info.key.as_ref(),
571                 "metadata".as_bytes(),
572             ],
573         )?;
574 
575         let bidder_pubkey =
        ↪  Pubkey::new_from_array(*array_ref![bidder_metadata_data, 0,
        ↪  32]);
```

```
576             if bidder_pubkey != *bidder_info.key {
577                 return Err(MetaplexError::BidderMetadataBidderMismatch.into());
578             }
579             let auction_key = auction_manager.auction();
580             let redemption_path = [
581                 PREFIX.as_bytes(),
582                 auction_key.as_ref(),
583                 bidder_metadata_info.key.as_ref(),
584             ];
585             let (redemption_key, actual_redemption_bump_seed) =
586                 Pubkey::find_program_address(&redemption_path, &program_id);
587
588             redemption_bump_seed = actual_redemption_bump_seed;
589             if redemption_key != *bid_redemption_info.key {
590                 return Err(MetaplexError::BidRedemptionMismatch.into());
591             }
592         }
593
594         let win_index = calculate_win_index(
595             bidder_info,
596             auction_info,
597             user_provided_win_index,
598             overwrite_win_index,
599         )?;
600
601         if !bid_redemption_info.data_is_empty()
602             && overwrite_win_index.is_none()
603             && !ignore_bid_redeemed_item_check
604         {
605             BidRedemptionTicket::check_ticket(
606                 bid_redemption_info,
607                 is_participation,
608                 safety_deposit_config_info,
609             )?
610         }
611
612         if assert_bidder_signer {
613             assert_signer(bidder_info)?;
614         }
615
616         assert_owned_by(&destination_info, token_program_info.key)?;
617         assert_owned_by(&auction_manager_info, &program_id)?;
```

```
618     assert_owned_by(safety_deposit_token_store_info,
    ↪ token_program_info.key)?;
619     if !bid_redemption_info.data_is_empty() {
620         assert_owned_by(bid_redemption_info, &program_id)?;
621     }
622     assert_owned_by(safety_deposit_info, &token_vault_program)?;
623     assert_owned_by(vault_info, &token_vault_program)?;
624     assert_owned_by(auction_info, &auction_program)?;
625     assert_owned_by(store_info, &program_id)?;
626
627     assert_store_safety_vault_manager_match(
628         &auction_manager.vault(),
629         &safety_deposit_info,
630         &vault_info,
631         &token_vault_program,
632     )?;
633     assert_safety_deposit_config_valid(
634         program_id,
635         auction_manager_info,
636         safety_deposit_info,
637         safety_deposit_config_info,
638         &auction_manager.key(),
639     )?;
640     // looking out for you!
641     assert_rent_exempt(rent, &destination_info)?;
642
643     if auction_manager.auction() != *auction_info.key {
644         return Err(MetaplexError::AuctionManagerAuctionMismatch.into());
645     }
646
647     if *store_info.key != auction_manager.store() {
648         return Err(MetaplexError::AuctionManagerStoreMismatch.into());
649     }
650
651     if token_program != *token_program_info.key {
652         return
        ↪ Err(MetaplexError::AuctionManagerTokenProgramMismatch.into());
653     }
654
655     if token_vault_program != *token_vault_program_info.key {
656         return
        ↪ Err(MetaplexError::AuctionManagerTokenVaultProgramMismatch.into());
```

```
657     }
658
659     if token_metadata_program != *token_metadata_program_info.key {
660         return
            ↪  Err(MetaplexError::AuctionManagerTokenMetadataProgramMismatch.into());
661     }
662
663     assert_auction_is_ended_or_valid_instant_sale(
664         auction_info,
665         auction_extended_info,
666         bidder_metadata_info,
667         win_index,
668     )?;
669
670     // No-op if already set.
671     auction_manager.set_status(AuctionManagerStatus::Disbursing);
672
673     Ok(CommonRedeemReturn {
674         redemption_bump_seed,
675         auction_manager,
676         cancelled,
677         rent: *rent,
678         win_index,
679         token_metadata_program,
680     })
681 }
682
```

- 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
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_6: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:190:5: 207:6

```
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             if data[bid_state_beginning] == 1 {
197                 bid_state_beginning += 9
198             } else {
199                 bid_state_beginning += 1;
200             }
201         }
202 
203         // Finally add price floor (enum + hash) and state, then the u32,
204         // then add 1 to position at the beginning of first bid.
205         bid_state_beginning += 1 + 32 + 1 + 4 + 1;
206         return bid_state_beginning;
207     }
208 
```

- 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(){//
                            ↪  /home/ubuntu/VRust/metaplex-program-
                            ↪  library/auction/program/src/processor.rs:221:5:
                            ↪  252:6 }
7                               fn
                                ↪  mpl_auction::processor::AuctionData::find_bid_state_begi
                                ↪  /home/ubuntu/VRust/metaplex-program-
                                ↪  library/auction/program/src/processor.rs:190:5:
                                ↪  207:6 }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_7: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:221:5: 252:6

```
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) =
        ↪  AuctionData::get_vec_info(a);
226         for idx in 0..std::cmp::min(num_elements, max) {
227             match AuctionData::get_winner_at_inner(
228                 &a.data.borrow(),
229                 idx,
230                 bid_state_beginning,
231                 num_elements,
232                 max,
233             ) {
234                 Some(bid_key) => {
235                     // why deserialize the entire key to compare the two
                        ↪  with a short circuit comparison
236                     // when we can compare them immediately?
237                     let mut matching = true;
238                     for bid_key_idx in 0..32 {
239                         if bid_key[bid_key_idx] != as_bytes[bid_key_idx] {
240                             matching = false;
241                             break;
242                         }
243                     }
244                     if matching {
245                         return Some(idx as usize);
246                     }
247                 }
248                 None => return None,
249             }
```

```
250         }
251         None
252     }
253
```

- 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(){//
                       ↪  /home/ubuntu/VRust/metaplex-program-
                       ↪  library/auction/program/src/processor.rs:221:5:
                       ↪  252:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_8: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:190:5: 207:6

```
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             if data[bid_state_beginning] == 1 {
197                 bid_state_beginning += 9
198             } else {
199                 bid_state_beginning += 1;
200             }
201         }
202 
203         // Finally add price floor (enum + hash) and state, then the u32,
204         // then add 1 to position at the beginning of first bid.
205         bid_state_beginning += 1 + 32 + 1 + 4 + 1;
206         return bid_state_beginning;
207     }
208 
```

- 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(){//
                        ↪  /home/ubuntu/VRust/metaplex-program-
                        ↪  library/auction/program/src/processor.rs:221:5:
                        ↪  252:6 }
7                           fn
                            ↪  mpl_auction::processor::AuctionData::get_vec_info(){//
                            ↪  /home/ubuntu/VRust/metaplex-program-
                            ↪  library/auction/program/src/processor.rs:209:5:
                            ↪  219:6 }
8       fn
        ↪  mpl_auction::processor::AuctionData::find_bid_state_beginning(){//
        ↪  /home/ubuntu/VRust/metaplex-program-
        ↪  library/auction/program/src/processor.rs:190:5: 207:6
        ↪  }
9
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_9: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:209:5: 219:6

```
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         let max = u64::from_le_bytes(*max_data) as usize;
217 
218         (bid_state_beginning, num_elements, max)
219     }
220 
```

- 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(){//
                       ↪  /home/ubuntu/VRust/metaplex-program-
                       ↪  library/auction/program/src/processor.rs:221:5:
                       ↪  252:6 }
```

```
7                                   fn
                                    ↪ mpl_auction::processor::AuctionData::get_vec_info(){//
                                    ↪ /home/ubuntu/VRust/metaplex-program-
                                    ↪ library/auction/program/src/processor.rs:209:5:
                                    ↪ 219:6 }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_10: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:190:5: 207:6

```
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             if data[bid_state_beginning] == 1 {
197                 bid_state_beginning += 9
198             } else {
199                 bid_state_beginning += 1;
200             }
201         }
202 
203         // Finally add price floor (enum + hash) and state, then the u32,
204         // then add 1 to position at the beginning of first bid.
205         bid_state_beginning += 1 + 32 + 1 + 4 + 1;
206         return bid_state_beginning;
207     }
208 
```

- 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_winner_at(){//
                        ↪  /home/ubuntu/VRust/metaplex-program-
                        ↪  library/auction/program/src/processor.rs:254:5:
                        ↪  266:6 }
7                           fn
                            ↪  mpl_auction::processor::AuctionData::get_vec_info(){//
                            ↪  /home/ubuntu/VRust/metaplex-program-
                            ↪  library/auction/program/src/processor.rs:209:5:
                            ↪  219:6 }
8       fn
        ↪  mpl_auction::processor::AuctionData::find_bid_state_beginning(){//
        ↪  /home/ubuntu/VRust/metaplex-program-
        ↪  library/auction/program/src/processor.rs:190:5: 207:6
        ↪  }
9
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_11: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:209:5: 219:6

```
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         let max = u64::from_le_bytes(*max_data) as usize;
217 
218         (bid_state_beginning, num_elements, max)
219     }
220 
```

- 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_winner_at(){//
                       ↪  /home/ubuntu/VRust/metaplex-program-
                       ↪  library/auction/program/src/processor.rs:254:5:
                       ↪  266:6 }
```

```
7                                   fn
                                    ↪ mpl_auction::processor::AuctionData::get_vec_info(){//
                                    ↪ /home/ubuntu/VRust/metaplex-program-
                                    ↪ library/auction/program/src/processor.rs:209:5:
                                    ↪ 219:6 }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_12: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:254:5: 266:6

```
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         ) {
263             Some(bid_key) => Some(Pubkey::new_from_array(*bid_key)),
264             None => None,
265         }
266     }
267
```

- 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_winner_at(){//
                        ↪ /home/ubuntu/VRust/metaplex-program-
                        ↪ library/auction/program/src/processor.rs:254:5:
                        ↪ 266:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_13: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 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 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:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_14: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/auction/program/src/processor.rs:167:5: 171:6

```
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(){//
               ↪  /home/ubuntu/VRust/metaplex-program-
               ↪  library/auction/program/src/processor.rs:167:5: 171:6
               ↪  }
5
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_15: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account_info.rs:101:5: 105:6

```
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/ubuntu/.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/ubuntu/.cargo/registry/src/github.com-
                   ↪  1ecc6299db9ec823/solana-program-
                   ↪  1.9.5/src/account_info.rs:101:5: 105:6
                   ↪  }
```

```
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_16: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.5/src/account_info.rs:101:5: 105:6

```
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 processor::redeem_participation_bid::v2_validation(){//
               ↪  meta-
               ↪  plex/program/src/processor/redeem_participation_bid.rs:65:1:
               ↪  129:2 }
5                 fn utils::get_amount_from_token_account(){//
                   ↪  metaplex/program/src/utils.rs:38:1: 45:2 }
6                     fn
                       ↪  solana_program::account_info::AccountInfo::<'a>::try_borrow_
                       ↪  /home/ubuntu/.cargo/registry/src/github.com-
                       ↪  1ecc6299db9ec823/solana-program-
                       ↪  1.9.5/src/account_info.rs:101:5: 105:6
                       ↪  }
```

```
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_17: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/processor/redeem_printing_v2_bid.rs:96:1: 165:2

```
96  pub fn create_or_update_prize_tracking<'a>(
97      program_id: &'a Pubkey,
98      auction_manager_info: &AccountInfo<'a>,
99      prize_tracking_ticket_info: &AccountInfo<'a>,
100     metadata_account_info: &AccountInfo<'a>,
101     payer_info: &AccountInfo<'a>,
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,
        ↪  33, 32]);
109
110     let bump = assert_derivation(
111         program_id,
112         prize_tracking_ticket_info,
113         &[
114             PREFIX.as_bytes(),
115             program_id.as_ref(),
116             auction_manager_info.key.as_ref(),
117             metadata_mint.as_ref(),
118         ],
119     )?;
120
121     let supply_snapshot: u64;
122     if prize_tracking_ticket_info.data_is_empty() {
123         create_or_allocate_account_raw(
124             *program_id,
125             prize_tracking_ticket_info,
```

```
126             rent_info,
127             system_info,
128             payer_info,
129             MAX_PRIZE_TRACKING_TICKET_SIZE,
130             &[
131                 PREFIX.as_bytes(),
132                 program_id.as_ref(),
133                 auction_manager_info.key.as_ref(),
134                 metadata_mint.as_ref(),
135                 &[bump],
136             ],
137         )?;
138         let data = &mut prize_tracking_ticket_info.data.borrow_mut();
139         let output = array_mut_ref![data, 0,
    ↪  MAX_PRIZE_TRACKING_TICKET_SIZE];
140 
141         let (key, metadata, supply_snapshot_ptr, expected_redemptions_ptr,
    ↪  redemptions, _padding) =
142             mut_array_refs![output, 1, 32, 8, 8, 8, 50];
143 
144         *key = [Key::PrizeTrackingTicketV1 as u8];
145         metadata.copy_from_slice(metadata_account_info.key.as_ref());
146         supply_snapshot =
↪   get_supply_off_master_edition(master_edition_account_info)?;
147         *supply_snapshot_ptr = supply_snapshot.to_le_bytes();
148         *redemptions = 1u64.to_le_bytes();
149         *expected_redemptions_ptr = expected_redemptions.to_le_bytes();
150     } else {
151         // CPU is very precious in this large action, so we skip borsh's
    ↪  angry CPU usage.
152         let data = &mut prize_tracking_ticket_info.data.borrow_mut();
153         let output = array_mut_ref![data, 0,
    ↪  MAX_PRIZE_TRACKING_TICKET_SIZE];
154 
155         let (_key, _metadata, supply_snapshot_ptr, _expected_redemptions,
    ↪  redemptions, _padding) =
156             mut_array_refs![output, 1, 32, 8, 8, 8, 50];
157         supply_snapshot = u64::from_le_bytes(*supply_snapshot_ptr);
158         let next_redemptions = u64::from_le_bytes(*redemptions)
159             .checked_add(1)
160             .ok_or(MetaplexError::NumericalOverflowError)?;
161         *redemptions = next_redemptions.to_le_bytes();
```

```
    }

    Ok(supply_snapshot)
}

```

- Call Stack

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

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_18: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/token-vault/program/src/state.rs:70:5: 72:6

```
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(){//
                      ↪  /home/ubuntu/VRust/metaplex-program-library/token-
                      ↪  vault/program/src/state.rs:70:5: 72:6
                      ↪  }
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_19: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 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 state::BidRedemptionTicket::save(){//
                       ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                         fn state::SafetyDepositConfig::get_order(){//
                           ↪  metaplex/program/src/state.rs:909:5: 912:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_20: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
          ↪  sor::redeem_printing_v2_bid::process_redeem_printing_v2_bid(){//
          ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
          ↪  350:2 }
4             fn utils::common_redeem_checks(){//
              ↪  metaplex/program/src/utils.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:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_21: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/token-vault/program/src/state.rs:70:5: 72:6

```
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_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
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(){//
                       ↪  /home/ubuntu/VRust/metaplex-program-library/token-
                       ↪  vault/program/src/state.rs:70:5: 72:6
                       ↪  }
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_22: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
           ↪  sor::redeem_printing_v2_bid::process_redeem_printing_v2_bid(){//
           ↪  metaplex/program/src/processor/redeem_printing_v2_bid.rs:167:1:
           ↪  350:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                     fn state::BidRedemptionTicket::save(){//
                       ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                         fn state::SafetyDepositConfig::get_order(){//
                           ↪  metaplex/program/src/state.rs:909:5: 912:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_23: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
          ↪  sor::redeem_unused_winning_config_items_as_auctioneer::process_redeem_unused
          ↪  meta-
          ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
          ↪  32:2 }
4             fn proces-
              ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
              ↪  meta-
              ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
              ↪  167:2 }
5                 fn utils::common_redeem_checks(){//
                  ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
6                     fn state::BidRedemptionTicket::check_ticket(){//
                      ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
7                         fn state::SafetyDepositConfig::get_order(){//
                          ↪  metaplex/program/src/state.rs:909:5: 912:6
                          ↪  }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_24: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/token-vault/program/src/state.rs:70:5: 72:6

```
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_unused_winning_config_items_as_auctioneer::process_redeem_unused
          ↪  meta-
          ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
          ↪  32:2 }
4             fn proces-
              ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
              ↪  meta-
              ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
              ↪  167:2 }
5                 fn utils::common_redeem_finish(){//
                  ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6                     fn
                      ↪  mpl_token_vault::state::Vault::get_token_type_count(){//
                      ↪  /home/ubuntu/VRust/metaplex-program-
                      ↪  library/token-vault/program/src/state.rs:70:5:
                      ↪  72:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_25: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
           ↪  sor::redeem_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn proces-
               ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid()
               ↪  meta-
               ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
               ↪  167:2 }
5                 fn utils::common_redeem_finish(){//
                   ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6                     fn state::BidRedemptionTicket::save(){//
                       ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
7                         fn state::SafetyDepositConfig::get_order(){//
                           ↪  metaplex/program/src/state.rs:909:5: 912:6
                           ↪  }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_26: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
           ↪  sor::redeem_unused_winning_config_items_as_auctioneer::process_redeem_unused
           ↪  meta-
           ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
           ↪  32:2 }
4             fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                 fn utils::common_redeem_checks(){//
                   ↪  metaplex/program/src/utils.rs:509:1: 681:2 }
6                     fn state::BidRedemptionTicket::check_ticket(){//
                       ↪  metaplex/program/src/state.rs:1476:5: 1520:6 }
7                         fn state::SafetyDepositConfig::get_order(){//
                           ↪  metaplex/program/src/state.rs:909:5: 912:6
                           ↪  }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_27: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/token-vault/program/src/state.rs:70:5: 72:6

```
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_unused_winning_config_items_as_auctioneer::process_redeem_unused
          ↪  meta-
          ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
          ↪  32:2 }
4             fn processor::redeem_bid::process_redeem_bid(){//
              ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                 fn utils::common_redeem_finish(){//
                  ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6                     fn
                      ↪  mpl_token_vault::state::Vault::get_token_type_count(){//
                      ↪  /home/ubuntu/VRust/metaplex-program-
                      ↪  library/token-vault/program/src/state.rs:70:5:
                      ↪  72:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_28: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
          ↪  sor::redeem_unused_winning_config_items_as_auctioneer::process_redeem_unused
          ↪  meta-
          ↪  plex/program/src/processor/redeem_unused_winning_config_items_as_auctioneer.
          ↪  32:2 }
4             fn processor::redeem_bid::process_redeem_bid(){//
               ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
5                 fn utils::common_redeem_finish(){//
                   ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
6                     fn state::BidRedemptionTicket::save(){//
                       ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
7                         fn state::SafetyDepositConfig::get_order(){//
                           ↪  metaplex/program/src/state.rs:909:5: 912:6
                           ↪  }
8
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_29: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
          ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
          ↪  meta-
          ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
          ↪  167:2 }
4             fn utils::common_redeem_checks(){//
               ↪  metaplex/program/src/utils.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:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_30: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/token-vault/program/src/state.rs:70:5: 72:6

```
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_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
          ↪  meta-
          ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
          ↪  167:2 }
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(){//
                  ↪  /home/ubuntu/VRust/metaplex-program-library/token-
                  ↪  vault/program/src/state.rs:70:5: 72:6
                  ↪  }
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_31: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 proces-
          ↪  sor::redeem_full_rights_transfer_bid::process_full_rights_transfer_bid(){//
          ↪  meta-
          ↪  plex/program/src/processor/redeem_full_rights_transfer_bid.rs:17:1:
          ↪  167:2 }
4             fn utils::common_redeem_finish(){//
               ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                     fn state::BidRedemptionTicket::save(){//
                       ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                         fn state::SafetyDepositConfig::get_order(){//
                           ↪  metaplex/program/src/state.rs:909:5: 912:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_32: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 processor::redeem_bid::process_redeem_bid(){//
          ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_checks(){//
              ↪  metaplex/program/src/utils.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:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_33: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/VRust/metaplex-program-library/token-vault/program/src/state.rs:70:5: 72:6

```
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 processor::redeem_bid::process_redeem_bid(){//
           ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
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(){//
                       ↪  /home/ubuntu/VRust/metaplex-program-library/token-
                       ↪  vault/program/src/state.rs:70:5: 72:6
                       ↪  }
6
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_34: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

metaplex/program/src/state.rs:909:5: 912:6

```
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 processor::redeem_bid::process_redeem_bid(){//
          ↪  metaplex/program/src/processor/redeem_bid.rs:125:1: 284:2 }
4             fn utils::common_redeem_finish(){//
              ↪  metaplex/program/src/utils.rs:702:1: 776:2 }
5                 fn state::BidRedemptionTicket::save(){//
                  ↪  metaplex/program/src/state.rs:1546:5: 1599:6 }
6                     fn state::SafetyDepositConfig::get_order(){//
                      ↪  metaplex/program/src/state.rs:909:5: 912:6 }
7
```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: CHK_CVE_0: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/deprecated_validate_participation.rs:24:1: 176:2

```
24 pub fn process_deprecated_validate_participation(
25     program_id: &Pubkey,
26     accounts: &[AccountInfo],
27 ) -> ProgramResult {
28     let account_info_iter = &mut accounts.iter();
29 
30     let auction_manager_info = next_account_info(account_info_iter)?;
31     let open_edition_metadata_info = next_account_info(account_info_iter)?;
32     let open_master_edition_info = next_account_info(account_info_iter)?;
33     let printing_authorization_token_account_info =
       ↪ next_account_info(account_info_iter)?;
34     let authority_info = next_account_info(account_info_iter)?;
35     let whitelisted_creator_info = next_account_info(account_info_iter)?;
36     let store_info = next_account_info(account_info_iter)?;
37     let safety_deposit_box_info = next_account_info(account_info_iter)?;
38     let safety_deposit_box_token_store_info =
       ↪ next_account_info(account_info_iter)?;
39     let vault_info = next_account_info(account_info_iter)?;
40     let rent_info = next_account_info(account_info_iter)?;
41     let rent = &Rent::from_account_info(&rent_info)?;
42 
43     let mut auction_manager =
       ↪ AuctionManagerV1::from_account_info(auction_manager_info)?;
44     let store = Store::from_account_info(store_info)?;
45     let vault = Vault::from_account_info(vault_info)?;
46     let safety_deposit_token_store: Account =
47         assert_initialized(safety_deposit_box_token_store_info)?;
48     let safety_deposit =
       ↪ SafetyDepositBox::from_account_info(safety_deposit_box_info)?;
```

```
49      let printing_token_account: Account =
50          assert_initialized(printing_authorization_token_account_info)?;
51      let open_edition_metadata =
        ↪ Metadata::from_account_info(open_edition_metadata_info)?;
52      let master_edition =
        ↪ MasterEditionV1::from_account_info(open_master_edition_info)?;
53
54      if vault.authority != *auction_manager_info.key {
55          return Err(MetaplexError::VaultAuthorityMismatch.into());
56      }
57
58      // top level authority and ownership check
59      assert_authority_correct(&auction_manager.authority, authority_info)?;
60      assert_owned_by(auction_manager_info, program_id)?;
61      assert_owned_by(open_edition_metadata_info,
    ↪ &store.token_metadata_program)?;
62      assert_owned_by(open_master_edition_info,
    ↪ &store.token_metadata_program)?;
63      assert_owned_by(
64          printing_authorization_token_account_info,
65          &store.token_program,
66      )?;
67      if *whitelisted_creator_info.key !=
        ↪ solana_program::system_program::id() {
68          if whitelisted_creator_info.data_is_empty() {
69              return Err(MetaplexError::Uninitialized.into());
70          }
71          assert_owned_by(whitelisted_creator_info, program_id)?;
72      }
73      assert_owned_by(store_info, program_id)?;
74      assert_owned_by(safety_deposit_box_info, &store.token_vault_program)?;
75      assert_owned_by(safety_deposit_box_token_store_info,
    ↪ &store.token_program)?;
76      assert_owned_by(vault_info, &store.token_vault_program)?;
77      // is it the right vault, safety deposit, and token store?
78      assert_store_safety_vault_manager_match(
79          &auction_manager.vault,
80          &safety_deposit_box_info,
81          vault_info,
82          &store.token_vault_program,
83      )?;
84
```

```
85      // do the vault and store belong to this AM?
86      if auction_manager.store != *store_info.key {
87          return Err(MetaplexError::AuctionManagerStoreMismatch.into());
88      }
89
90      if auction_manager.vault != *vault_info.key {
91          return Err(MetaplexError::AuctionManagerVaultMismatch.into());
92      }
93      // Check creators
94      assert_at_least_one_creator_matches_or_store_public_and_all_verified(
95          program_id,
96          &auction_manager,
97          &open_edition_metadata,
98          whitelisted_creator_info,
99          store_info,
100     )?;
101
102     // Make sure master edition is the right master edition for this
        ↪ metadata given
103     assert_derivation(
104         &store.token_metadata_program,
105         open_master_edition_info,
106         &[
107             mpl_token_metadata::state::PREFIX.as_bytes(),
108             store.token_metadata_program.as_ref(),
109             &open_edition_metadata.mint.as_ref(),
110             mpl_token_metadata::state::EDITION.as_bytes(),
111         ],
112     )?;
113
114     // Assert the holding account for authorization tokens is rent filled,
        ↪ owned correctly, and ours
115     assert_owned_by(
116         printing_authorization_token_account_info,
117         &store.token_program,
118     )?;
119     assert_rent_exempt(rent, printing_authorization_token_account_info)?;
120
121     if printing_token_account.owner != *auction_manager_info.key {
122         return Err(MetaplexError::IncorrectOwner.into());
123     }
124
```

```
125     if printing_token_account.mint != master_edition.printing_mint {
126         return Err(MetaplexError::PrintingTokenAccountMintMismatch.into());
127     }
128
129     if printing_token_account.delegate != COption::None {
130         return Err(MetaplexError::DelegateShouldBeNone.into());
131     }
132
133     if printing_token_account.close_authority != COption::None {
134         return Err(MetaplexError::CloseAuthorityShouldBeNone.into());
135     }
136
137     if master_edition.max_supply.is_some() {
138         return
        ↪  Err(MetaplexError::CantUseLimitedSupplyEditionsWithOpenEditionAuction.into()
139     }
140
141     if master_edition.one_time_printing_authorization_mint !=
    ↪  safety_deposit_token_store.mint {
142         return
        ↪  Err(MetaplexError::MasterEditionOneTimeAuthorizationMintMismatch.into());
143     }
144
145     if let Some(participation_config) =
    ↪  &auction_manager.settings.participation_config {
146         if participation_config.safety_deposit_box_index >
        ↪  vault.token_type_count {
147             return Err(MetaplexError::InvalidSafetyDepositBox.into());
148         }
149
150         if participation_config.safety_deposit_box_index !=
        ↪  safety_deposit.order {
151             return Err(MetaplexError::SafetyDepositIndexMismatch.into());
152         }
153
154         if let Some(state) = auction_manager.state.participation_state {
155             if state.validated {
156                 return Err(MetaplexError::AlreadyValidated.into());
157             }
158
159             auction_manager.state.participation_state =
↪   Some(ParticipationStateV1 {
```

```
                collected_to_accept_payment:
↪   state.collected_to_accept_payment,
                primary_sale_happened:
↪   open_edition_metadata.primary_sale_happened,
                validated: true,
                printing_authorization_token_account: Some(
                    *printing_authorization_token_account_info.key,
                ),
            });
        }

        if auction_manager.settings.winning_configs.is_empty() {
            auction_manager.state.status = AuctionManagerStatus::Validated;
        }
        auction_manager.serialize(&mut
↪   *auction_manager_info.data.borrow_mut())?;
    }

    Ok(())
}

```

- Call Stack

```
processor::deprecated_validate_participation::process_deprecated_validate_participation
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_1: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

`Todo: Add owner variable`

- Location

metaplex/program/src/processor/deprecated_validate_safety_deposit_box_v1.rs:67:1: 237:2

```
67 pub fn process_deprecated_validate_safety_deposit_box_v1<'a>(
68     program_id: &'a Pubkey,
69     accounts: &'a [AccountInfo<'a>],
70 ) -> ProgramResult {
71     let account_info_iter = &mut accounts.iter();
72     let safety_deposit_validation_ticket_info =
       ↪  next_account_info(account_info_iter)?;
73     let auction_manager_info = next_account_info(account_info_iter)?;
74     let metadata_info = next_account_info(account_info_iter)?;
75     let original_authority_lookup_info =
       ↪  next_account_info(account_info_iter)?;
76     let whitelisted_creator_info = next_account_info(account_info_iter)?;
77     let auction_manager_store_info = next_account_info(account_info_iter)?;
78     let safety_deposit_info = next_account_info(account_info_iter)?;
79     let safety_deposit_token_store_info =
       ↪  next_account_info(account_info_iter)?;
80     let mint_info = next_account_info(account_info_iter)?;
81     let edition_info = next_account_info(account_info_iter)?;
82     let vault_info = next_account_info(account_info_iter)?;
83     let authority_info = next_account_info(account_info_iter)?;
84     let metadata_authority_info = next_account_info(account_info_iter)?;
85     let payer_info = next_account_info(account_info_iter)?;
86     let token_metadata_program_info =
       ↪  next_account_info(account_info_iter)?;
87     let system_info = next_account_info(account_info_iter)?;
88     let rent_info = next_account_info(account_info_iter)?;
89
90     if !safety_deposit_validation_ticket_info.data_is_empty() {
```

```
91          return Err(MetaplexError::AlreadyValidated.into());
92      }
93
94      let mut auction_manager =
        ↪  AuctionManagerV1::from_account_info(auction_manager_info)?;
95      let safety_deposit =
        ↪  SafetyDepositBox::from_account_info(safety_deposit_info)?;
96      let _safety_deposit_token_store: Account =
        ↪  assert_initialized(safety_deposit_token_store_info)?;
97      let metadata = Metadata::from_account_info(metadata_info)?;
98      let store = Store::from_account_info(auction_manager_store_info)?;
99      // Is it a real vault?
100     let vault = Vault::from_account_info(vault_info)?;
101
102     let mut total_amount_requested: u64 = 0;
103     // At this point we know we have at least one config and they may have
        ↪  different amounts but all
104     // point at the same safety deposit box and so have the same winning
        ↪  config type.
105     // We default to TokenOnlyTransfer but this will get set by the loop.
106     let mut winning_config_type: WinningConfigType =
        ↪  WinningConfigType::TokenOnlyTransfer;
107     let mut winning_config_items_validated: u8 = 0;
108     let mut all_winning_config_items: u8 = 0;
109
110     for i in 0..auction_manager.settings.winning_configs.len() {
111         let possible_config = &auction_manager.settings.winning_configs[i];
112
113         for j in 0..possible_config.items.len() {
114             let possible_item = &possible_config.items[j];
115             all_winning_config_items = all_winning_config_items
116                 .checked_add(1)
117                 .ok_or(MetaplexError::NumericalOverflowError)?;
118
119             if possible_item.safety_deposit_box_index ==
                ↪  safety_deposit.order {
120                 winning_config_type = possible_item.winning_config_type;
121
122                 winning_config_items_validated =
↪   winning_config_items_validated
123                     .checked_add(1)
124                     .ok_or(MetaplexError::NumericalOverflowError)?;
```

```
125
126                 // Build array to sum total amount
127                 total_amount_requested = total_amount_requested
128                     .checked_add(possible_item.amount.into())
129                     .ok_or(MetaplexError::NumericalOverflowError)?;
130                 // Record that primary sale happened at time of validation
                    ↪  for later royalties reconcilation
131                 auc-
    ↪  tion_manager.state.winning_config_states[i].items[j].primary_sale_happened
    ↪  =
132                     metadata.primary_sale_happened;
133             }
134         }
135     }
136
137     if let Some(participation_config) =
        ↪  &auction_manager.settings.participation_config {
138         if participation_config.safety_deposit_box_index ==
            ↪  safety_deposit.order {
139             // Really it's unknown how many prints will be made
140             // but we set it to 1 since that's how many master edition
                ↪  tokens are in there.
141             total_amount_requested = total_amount_requested
142                 .checked_add(1)
143                 .ok_or(MetaplexError::NumericalOverflowError)?;
144
145             // now that participation configs can be validated through
                ↪  normal safety deposit endpoints, need to flip this boolean
146             // here too, until we can deprecate it later.
147             if let Some(state) = &auction_manager.state.participation_state
                ↪  {
148                 auction_manager.state.participation_state =
    ↪  Some(ParticipationStateV1 {
149                     collected_to_accept_payment:
    ↪  state.collected_to_accept_payment,
150                     primary_sale_happened: state.primary_sale_happened,
151                     validated: true,
152                     printing_authorization_token_account: state
153                         .printing_authorization_token_account,
154                 })
155             }
156         }
```

```
157     }
158
159     if total_amount_requested == 0 {
160         return Err(MetaplexError::SafetyDepositBoxNotUsedInAuction.into());
161     }
162
163     assert_common_checks(CommonCheckArgs {
164         program_id,
165         auction_manager_info,
166         metadata_info,
167         original_authority_lookup_info,
168         whitelisted_creator_info,
169         safety_deposit_info,
170         safety_deposit_token_store_info,
171         edition_info,
172         vault_info,
173         mint_info,
174         token_metadata_program_info,
175         auction_manager_store_info,
176         authority_info,
177         store: &store,
178         auction_manager: &auction_manager,
179         metadata: &metadata,
180         safety_deposit: &safety_deposit,
181         vault: &vault,
182         winning_config_type: &winning_config_type,
183     })?;
184
185     assert_supply_logic_check(SupplyLogicCheckArgs {
186         program_id,
187         auction_manager_info,
188         metadata_info,
189         edition_info,
190         metadata_authority_info,
191         original_authority_lookup_info,
192         rent_info,
193         system_info,
194         payer_info,
195         token_metadata_program_info,
196         auction_manager: &auction_manager,
197         winning_config_type: &winning_config_type,
198         metadata: &metadata,
```

```
199         safety_deposit: &safety_deposit,
200         store: &store,
201         safety_deposit_token_store_info,
202         total_amount_requested,
203     })?;
204
205     auction_manager.state.winning_config_items_validated = match
    ↪   auction_manager
206         .state
207         .winning_config_items_validated
208         .checked_add(winning_config_items_validated)
209     {
210         Some(val) => val,
211         None => return Err(MetaplexError::NumericalOverflowError.into()),
212     };
213
214     if auction_manager.state.winning_config_items_validated ==
    ↪   all_winning_config_items {
215         let mut participation_okay = true;
216         if let Some(state) = &auction_manager.state.participation_state {
217             participation_okay = state.validated
218         }
219         if participation_okay {
220             auction_manager.state.status = AuctionManagerStatus::Validated
221         }
222     }
223
224     auction_manager.serialize(&mut
    ↪   *auction_manager_info.data.borrow_mut())?;
225
226     make_safety_deposit_validation(
227         program_id,
228         auction_manager_info,
229         safety_deposit_info,
230         safety_deposit_validation_ticket_info,
231         payer_info,
232         rent_info,
233         system_info,
234     )?;
235
236     Ok(())
237 }
```

```
238
```

- Call Stack

```
processor::deprecated_validate_safety_deposit_box_v1::process_deprecated_validate_safety
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_2: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

`Todo: Add owner variable`

- Location

metaplex/program/src/processor/empty_payment_account.rs:212:1: 458:2

```
212 pub fn process_empty_payment_account(
213     program_id: &Pubkey,
214     accounts: &[AccountInfo],
215     args: EmptyPaymentAccountArgs,
216 ) -> ProgramResult {
217     let account_info_iter = &mut accounts.iter();
218     let accept_payment_info = next_account_info(account_info_iter)?;
219     let destination_info = next_account_info(account_info_iter)?;
220     let auction_manager_info = next_account_info(account_info_iter)?;
221     let payout_ticket_info = next_account_info(account_info_iter)?;
222     let payer_info = next_account_info(account_info_iter)?;
223     let metadata_info = next_account_info(account_info_iter)?;
224     let master_edition_info = next_account_info(account_info_iter)?;
225     let safety_deposit_info = next_account_info(account_info_iter)?;
226     let store_info = next_account_info(account_info_iter)?;
227     let vault_info = next_account_info(account_info_iter)?;
228     let auction_info = next_account_info(account_info_iter)?;
229     let token_program_info = next_account_info(account_info_iter)?;
230     let system_info = next_account_info(account_info_iter)?;
231     let rent_info = next_account_info(account_info_iter)?;
232     let auction_token_tracker_info =
      ↪  next_account_info(account_info_iter).ok();
233     let safety_deposit_config_info =
      ↪  next_account_info(account_info_iter).ok();
234
235     if let Some(tracker_info) = auction_token_tracker_info {
236         assert_derivation(
237             program_id,
```

```
238             tracker_info,
239             &[
240                 PREFIX.as_bytes(),
241                 &program_id.as_ref(),
242                 auction_manager_info.key.as_ref(),
243                 TOTALS.as_bytes(),
244             ],
245         )?;
246     }
247
248     let rent = &Rent::from_account_info(&rent_info)?;
249
250     let auction_manager = get_auction_manager(auction_manager_info)?;
251     let store = Store::from_account_info(store_info)?;
252     let safety_deposit =
    ↪  SafetyDepositBox::from_account_info(safety_deposit_info)?;
253     let metadata = Metadata::from_account_info(metadata_info)?;
254     let auction = AuctionData::from_account_info(auction_info)?;
255     let destination: Account = assert_initialized(destination_info)?;
256     let accept_payment: Account = assert_initialized(accept_payment_info)?;
257
258     if auction_manager.store() != *store_info.key {
259         return Err(MetaplexError::AuctionManagerStoreMismatch.into());
260     }
261
262     msg!(
263         "At this point, accept payment has {:?} in it",
264         accept_payment.amount
265     );
266
267     // Before continuing further, assert all bid monies have been pushed to
    ↪  the main escrow
268     // account so that we have a complete (less the unredeemed
    ↪  participation nft bids) accounting
269     // to work with
270     auction_manager.assert_all_bids_claimed(&auction)?;
271
272     if *token_program_info.key != store.token_program {
273         return
        ↪  Err(MetaplexError::AuctionManagerTokenProgramMismatch.into());
274     }
275
```

```
276     assert_owned_by(auction_manager_info, program_id)?;
277     if !payout_ticket_info.data_is_empty() {
278         assert_owned_by(payout_ticket_info, program_id)?;
279     }
280     assert_owned_by(destination_info, token_program_info.key)?;
281     assert_owned_by(accept_payment_info, token_program_info.key)?;
282     assert_owned_by(metadata_info, &store.token_metadata_program)?;
283     if *master_edition_info.key != solana_program::system_program::id() {
284         assert_owned_by(master_edition_info,
    ↪ &store.token_metadata_program)?;
285     }
286     assert_owned_by(safety_deposit_info, &store.token_vault_program)?;
287     assert_owned_by(store_info, program_id)?;
288     assert_owned_by(vault_info, &store.token_vault_program)?;
289     assert_owned_by(auction_info, &store.auction_program)?;
290     assert_rent_exempt(rent, destination_info)?;
291
292     // Assert the winning config points to the safety deposit you sent up
293     auction_manager.assert_winning_config_safety_deposit_validity(
294         &safety_deposit,
295         args.winning_config_index,
296         args.winning_config_item_index,
297     )?;
298
299     assert_safety_deposit_config_valid(
300         program_id,
301         auction_manager_info,
302         safety_deposit_info,
303         safety_deposit_config_info,
304         &auction_manager.key(),
305     )?;
306
307     // assert the destination account matches the ownership expected to
    ↪  creator or auction manager authority
308     // given in the argument's creator index
309     assert_destination_ownership_validity(
310         &auction_manager,
311         &metadata,
312         destination_info,
313         &destination,
314         &store,
315         args.creator_index,
```

```
316     )?;
317
318     // further assert that the vault and safety deposit are correctly
        ↪  matched to the auction manager
319     if auction_manager.vault() != *vault_info.key {
320         return Err(MetaplexError::AuctionManagerVaultMismatch.into());
321     }
322
323     if auction_manager.auction() != *auction_info.key {
324         return Err(MetaplexError::AuctionManagerAuctionMismatch.into());
325     }
326
327     if safety_deposit.vault != *vault_info.key {
328         return Err(MetaplexError::SafetyDepositBoxVaultMismatch.into());
329     }
330
331     // assert that the metadata sent up is the metadata in the safety
        ↪  deposit
332     if metadata.mint != safety_deposit.token_mint {
333         if master_edition_info.data.borrow()[0]
334             == mpl_token_metadata::state::Key::MasterEditionV1 as u8
335         {
336             // Could be a limited edition, in which case printing tokens or
                ↪  auth tokens were offered, not the original.
337             let master_edition: MasterEditionV1 =
338                 MasterEditionV1::from_account_info(master_edition_info)?;
339             if master_edition.printing_mint != safety_deposit.token_mint
340                 && master_edition.one_time_printing_authorization_mint !=
↪   safety_deposit.token_mint
341             {
342                 return
                    ↪  Err(MetaplexError::SafetyDepositBoxMetadataMismatch.into());
343             }
344         } else {
345             return
                ↪  Err(MetaplexError::SafetyDepositBoxMetadataMismatch.into());
346         }
347     }
348
349     // make sure the accept payment account is right
350     if auction_manager.accept_payment() != *accept_payment_info.key {
351         return Err(MetaplexError::AcceptPaymentMismatch.into());
```

```
352     }
353
354     if destination.mint != accept_payment.mint {
355         return Err(MetaplexError::AcceptPaymentMintMismatch.into());
356     }
357
358     let winning_config_index_key: String = match args.winning_config_index
        ↪ {
359         Some(val) => val.to_string(),
360         None => "participation".to_owned(),
361     };
362
363     let winning_config_item_index_key: String = match
        ↪ args.winning_config_item_index {
364         Some(val) => val.to_string(),
365         None => "0".to_owned(),
366     };
367
368     let creator_index_key: String = match args.creator_index {
369         Some(val) => val.to_string(),
370         None => "auctioneer".to_owned(),
371     };
372
373     let payout_bump = assert_derivation(
374         program_id,
375         payout_ticket_info,
376         &[
377             PREFIX.as_bytes(),
378             auction_manager_info.key.as_ref(),
379             winning_config_index_key.as_bytes(),
380             winning_config_item_index_key.as_bytes(),
381             creator_index_key.as_bytes(),
382             &safety_deposit_info.key.as_ref(),
383             &destination.owner.as_ref(),
384         ],
385     )?;
386
387     let payout_seeds = &[
388         PREFIX.as_bytes(),
389         auction_manager_info.key.as_ref(),
390         winning_config_index_key.as_bytes(),
391         winning_config_item_index_key.as_bytes(),
```

```
392         creator_index_key.as_bytes(),
393         &safety_deposit_info.key.as_ref(),
394         &destination.owner.as_ref(),
395         &[payout_bump],
396     ];
397
398     if payout_ticket_info.data_is_empty() {
399         create_or_allocate_account_raw(
400             *program_id,
401             payout_ticket_info,
402             rent_info,
403             system_info,
404             payer_info,
405             MAX_PAYOUT_TICKET_SIZE,
406             payout_seeds,
407         )?;
408     }
409
410     let mut payout_ticket =
    ↪  PayoutTicket::from_account_info(payout_ticket_info)?;
411     payout_ticket.recipient = destination.owner;
412     payout_ticket.key = Key::PayoutTicketV1;
413
414     let amount = calculate_owed_amount(
415         auction_token_tracker_info,
416         safety_deposit_config_info,
417         &auction_manager,
418         &auction,
419         &metadata,
420         &args.winning_config_index,
421         &args.winning_config_item_index,
422         &args.creator_index,
423     )?;
424
425     let final_amount = amount
426         .checked_sub(payout_ticket.amount_paid)
427         .ok_or(MetaplexError::NumericalOverflowError)?;
428
429     if final_amount > 0 {
430         payout_ticket.amount_paid = payout_ticket
431             .amount_paid
432             .checked_add(final_amount)
```

```
            .ok_or(MetaplexError::NumericalOverflowError)?;

        let auction_key = auction_manager.auction();

        let bump_seed = assert_derivation(
            program_id,
            auction_manager_info,
            &[PREFIX.as_bytes(), auction_key.as_ref()],
        )?;

        let authority_seeds = &[PREFIX.as_bytes(), auction_key.as_ref(),
        ↪  &[bump_seed]];

        spl_token_transfer(
            accept_payment_info.clone(),
            destination_info.clone(),
            final_amount,
            auction_manager_info.clone(),
            authority_seeds,
            token_program_info.clone(),
        )?;
    }

    payout_ticket.serialize(&mut *payout_ticket_info.data.borrow_mut())?;

    Ok(())
}

```

- Call Stack

```
processor::empty_payment_account::process_empty_payment_account
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_3: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/validate_safety_deposit_box_v2.rs:205:1: 381:2

```
205 pub fn assert_supply_logic_check(args: SupplyLogicCheckArgs) ->
    ↪ ProgramResult {
206     let SupplyLogicCheckArgs {
207         program_id,
208         auction_manager_info,
209         metadata_info,
210         edition_info,
211         metadata_authority_info,
212         original_authority_lookup_info,
213         rent_info,
214         system_info,
215         payer_info,
216         token_metadata_program_info,
217         auction_manager,
218         winning_config_type,
219         metadata,
220         safety_deposit,
221         store,
222         safety_deposit_token_store_info,
223         total_amount_requested,
224     } = args;
225
226     let safety_deposit_token_store: Account =
        ↪ assert_initialized(safety_deposit_token_store_info)?;
227
228     let edition_seeds = &[
229         mpl_token_metadata::state::PREFIX.as_bytes(),
230         store.token_metadata_program.as_ref(),
```

```
231         &metadata.mint.as_ref(),
232         mpl_token_metadata::state::EDITION.as_bytes(),
233     ];
234
235     let (edition_key, _) =
236         Pubkey::find_program_address(edition_seeds,
            ↪  &store.token_metadata_program);
237
238     let auction_key = auction_manager.auction();
239     let seeds = &[PREFIX.as_bytes(), auction_key.as_ref()];
240     let (_, bump_seed) = Pubkey::find_program_address(seeds, &program_id);
241     let authority_seeds = &[PREFIX.as_bytes(), auction_key.as_ref(),
        ↪  &[bump_seed]];
242     // Supply logic check
243     match winning_config_type {
244         WinningConfigType::FullRightsTransfer => {
245             assert_update_authority_is_correct(&metadata,
↪   metadata_authority_info)?;
246
247             if safety_deposit.token_mint != metadata.mint {
248                 return
                    ↪  Err(MetaplexError::SafetyDepositBoxMetadataMismatch.into());
249             }
250             if edition_key != *edition_info.key {
251                 return Err(MetaplexError::InvalidEditionAddress.into());
252             }
253
254             if safety_deposit_token_store.amount != 1 {
255                 return Err(MetaplexError::StoreIsEmpty.into());
256             }
257
258             if total_amount_requested != 1 {
259                 return
                    ↪  Err(MetaplexError::NotEnoughTokensToSupplyWinners.into());
260             }
261
262             let auction_key = auction_manager.auction();
263
264             let original_authority_lookup_seeds = &[
265                 PREFIX.as_bytes(),
266                 auction_key.as_ref(),
267                 metadata_info.key.as_ref(),
```

```
268             ];
269
270             let (expected_key, original_bump_seed) =
271                 Pub-
                    ↪ key::find_program_address(original_authority_lookup_seeds,
                    ↪ &program_id);
272             let original_authority_seeds = &[
273                 PREFIX.as_bytes(),
274                 auction_key.as_ref(),
275                 metadata_info.key.as_ref(),
276                 &[original_bump_seed],
277             ];
278
279             if expected_key != *original_authority_lookup_info.key {
280                 return
                    ↪ Err(MetaplexError::OriginalAuthorityLookupKeyMismatch.into());
281             }
282
283             // We may need to transfer authority back, or to the new owner,
                ↪ so we need to keep track
284             // of original ownership
285             create_or_allocate_account_raw(
286                 *program_id,
287                 original_authority_lookup_info,
288                 rent_info,
289                 system_info,
290                 payer_info,
291                 MAX_AUTHORITY_LOOKUP_SIZE,
292                 original_authority_seeds,
293             )?;
294
295             let mut original_authority_lookup =
296                 OriginalAuthority-
                    ↪ Lookup::from_account_info(original_authority_lookup_info)?;
297             original_authority_lookup.key = Key::OriginalAuthorityLookupV1;
298
299             original_authority_lookup.original_authority =
↪   *metadata_authority_info.key;
300
301             transfer_metadata_ownership(
302                 token_metadata_program_info.clone(),
303                 metadata_info.clone(),
```

```
304                 metadata_authority_info.clone(),
305                 auction_manager_info.clone(),
306                 authority_seeds,
307             )?;
308
309             original_authority_lookup
310                 .serialize(&mut
    ↪  *original_authority_lookup_info.data.borrow_mut())?;
311         }
312         WinningConfigType::TokenOnlyTransfer => {
313             if safety_deposit.token_mint != metadata.mint {
314                 return
                     ↪  Err(MetaplexError::SafetyDepositBoxMetadataMismatch.into());
315             }
316             if safety_deposit_token_store.amount < total_amount_requested {
317                 return
                     ↪  Err(MetaplexError::NotEnoughTokensToSupplyWinners.into());
318             }
319         }
320         WinningConfigType::PrintingV1 => {
321             if edition_key != *edition_info.key {
322                 return Err(MetaplexError::InvalidEditionAddress.into());
323             }
324             let master_edition =
                 ↪  MasterEditionV1::from_account_info(edition_info)?;
325             if safety_deposit.token_mint != master_edition.printing_mint {
326                 return
                     ↪  Err(MetaplexError::SafetyDepositBoxMasterMintMismatch.into());
327             }
328
329             if safety_deposit_token_store.amount != total_amount_requested
                 ↪  {
330                 return
                     ↪  Err(MetaplexError::NotEnoughTokensToSupplyWinners.into());
331             }
332         }
333         WinningConfigType::PrintingV2 => {
334             if edition_key != *edition_info.key {
335                 return Err(MetaplexError::InvalidEditionAddress.into());
336             }
337             let master_edition =
                 ↪  MasterEditionV2::from_account_info(edition_info)?;
```

```
338             if safety_deposit.token_mint != metadata.mint {
339                 return
                    ↪  Err(MetaplexError::SafetyDepositBoxMetadataMismatch.into());
340             }
341
342             if safety_deposit_token_store.amount != 1 {
343                 return
                    ↪  Err(MetaplexError::NotEnoughTokensToSupplyWinners.into());
344             }
345
346             if let Some(max) = master_edition.max_supply {
347                 let amount_available = max
348                     .checked_sub(master_edition.supply)
349                     .ok_or(MetaplexError::NumericalOverflowError)?;
350                 if amount_available < total_amount_requested {
351                     return
                        ↪  Err(MetaplexError::NotEnoughTokensToSupplyWinners.into());
352                 }
353             }
354         }
355         WinningConfigType::Participation => {
356             // Impossible to use a MEV1 through this avenue of
                ↪  participation...no one time auth token allowed here...
357             // If you wish to use those, you must use the AuctionManagerV1
                ↪  pathway which allows use of the older endpoints,
358             // which will classify Participation as a PrintingV2 if it's an
                ↪  MEv2 or use the validate_participation endpoint
359             // if it's an MEv1.
360             if edition_key != *edition_info.key {
361                 return Err(MetaplexError::InvalidEditionAddress.into());
362             }
363             let master_edition =
                ↪  MasterEditionV2::from_account_info(edition_info)?;
364             if safety_deposit.token_mint != metadata.mint {
365                 return
                    ↪  Err(MetaplexError::SafetyDepositBoxMetadataMismatch.into());
366             }
367
368             if safety_deposit_token_store.amount != 1 {
369                 return
                    ↪  Err(MetaplexError::NotEnoughTokensToSupplyWinners.into());
370             }
```

```
371
372             if master_edition.max_supply.is_some() {
373                 return Err(
374                     MetaplexEr-
                        ↪ ror::CantUseLimitedSupplyEditionsWithOpenEditionAuction.into(),
375                 );
376             }
377         }
378     }
379
380     Ok(())
381 }
382
```

- Call Stack

```
1 processor::validate_safety_deposit_box_v2::assert_supply_logic_check
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_4: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/set_whitelisted_creator.rs:16:1: 84:2

```
16 pub fn process_set_whitelisted_creator<'a>(
17     program_id: &'a Pubkey,
18     accounts: &'a [AccountInfo<'a>],
19     activated: bool,
20 ) -> ProgramResult {
21     let account_info_iter = &mut accounts.iter();
22 
23     let whitelisted_creator_info = next_account_info(account_info_iter)?;
24     let admin_wallet_info = next_account_info(account_info_iter)?;
25     let payer_info = next_account_info(account_info_iter)?;
26     let creator_info = next_account_info(account_info_iter)?;
27     let store_info = next_account_info(account_info_iter)?;
28     let system_info = next_account_info(account_info_iter)?;
29     let rent_info = next_account_info(account_info_iter)?;
30 
31     assert_signer(payer_info)?;
32     assert_signer(admin_wallet_info)?;
33     if !whitelisted_creator_info.data_is_empty() {
34         assert_owned_by(whitelisted_creator_info, program_id)?;
35     }
36     assert_owned_by(store_info, program_id)?;
37 
38     assert_derivation(
39         program_id,
40         store_info,
41         &[
42             PREFIX.as_bytes(),
43             program_id.as_ref(),
```

```
            admin_wallet_info.key.as_ref(),
        ],
    )?;

    let creator_bump = assert_derivation(
        program_id,
        whitelisted_creator_info,
        &[
            PREFIX.as_bytes(),
            program_id.as_ref(),
            store_info.key.as_ref(),
            creator_info.key.as_ref(),
        ],
    )?;

    if whitelisted_creator_info.data_is_empty() {
        create_or_allocate_account_raw(
            *program_id,
            whitelisted_creator_info,
            rent_info,
            system_info,
            payer_info,
            MAX_WHITELISTED_CREATOR_SIZE,
            &[
                PREFIX.as_bytes(),
                program_id.as_ref(),
                store_info.key.as_ref(),
                creator_info.key.as_ref(),
                &[creator_bump],
            ],
        )?;
    }

    let mut whitelisted_creator =
    ↪  WhitelistedCreator::from_account_info(whitelisted_creator_info)?;
    whitelisted_creator.key = Key::WhitelistedCreatorV1;
    whitelisted_creator.address = *creator_info.key;
    whitelisted_creator.activated = activated;

    whitelisted_creator.serialize(&mut
↪   *whitelisted_creator_info.data.borrow_mut())?;
    Ok(())
```

```
}

```

- Call Stack

```
processor::set_whitelisted_creator::process_set_whitelisted_creator
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_5: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/set_store_index.rs:22:1: 217:2

```
22 pub fn process_set_store_index<'a>(
23     program_id: &'a Pubkey,
24     accounts: &'a [AccountInfo<'a>],
25     args: SetStoreIndexArgs,
26 ) -> ProgramResult {
27     let SetStoreIndexArgs { offset, page } = args;
28 
29     let offset_u = offset as usize;
30 
31     let account_info_iter = &mut accounts.iter();
32 
33     let store_index_info = next_account_info(account_info_iter)?;
34     let payer_info = next_account_info(account_info_iter)?;
35     let auction_cache_info = next_account_info(account_info_iter)?;
36     let store_info = next_account_info(account_info_iter)?;
37     let system_info = next_account_info(account_info_iter)?;
38     let rent_info = next_account_info(account_info_iter)?;
39     let above_cache_info = next_account_info(account_info_iter).ok();
40     let below_cache_info = next_account_info(account_info_iter).ok();
41     let _store = Store::from_account_info(store_info)?;
42     let auction_cache =
       ↪  AuctionCache::from_account_info(auction_cache_info)?;
43 
44     let mut below_cache: Option<AuctionCache> = None;
45     let mut above_cache: Option<AuctionCache> = None;
46 
47     assert_signer(payer_info)?;
48     assert_owned_by(store_info, program_id)?;
```

```
49      assert_owned_by(auction_cache_info, program_id)?;
50
51      if system_info.key != &solana_program::system_program::id() {
52          return Err(MetaplexError::InvalidSystemProgram.into());
53      }
54
55      assert_derivation(
56          program_id,
57          auction_cache_info,
58          &[
59              PREFIX.as_bytes(),
60              program_id.as_ref(),
61              store_info.key.as_ref(),
62              auction_cache.auction.as_ref(),
63              CACHE.as_bytes(),
64          ],
65      )?;
66
67      if let Some(below) = below_cache_info {
68          let unwrapped = AuctionCache::from_account_info(below)?;
69
70          assert_derivation(
71              program_id,
72              below,
73              &[
74                  PREFIX.as_bytes(),
75                  program_id.as_ref(),
76                  store_info.key.as_ref(),
77                  unwrapped.auction.as_ref(),
78                  CACHE.as_bytes(),
79              ],
80          )?;
81          assert_owned_by(below, program_id)?;
82
83          below_cache = Some(unwrapped);
84      }
85
86      if let Some(above) = &above_cache_info {
87          let unwrapped = AuctionCache::from_account_info(above)?;
88
89          assert_derivation(
90              program_id,
```

```
            above,
            &[
                PREFIX.as_bytes(),
                program_id.as_ref(),
                store_info.key.as_ref(),
                unwrapped.auction.as_ref(),
                CACHE.as_bytes(),
            ],
        )?;
        assert_owned_by(above, program_id)?;

        above_cache = Some(unwrapped);
    }

    let as_string = page.to_string();
    let bump = assert_derivation(
        program_id,
        store_index_info,
        &[
            PREFIX.as_bytes(),
            program_id.as_ref(),
            store_info.key.as_ref(),
            INDEX.as_bytes(),
            as_string.as_bytes(),
        ],
    )?;

    if store_index_info.data_is_empty() {
        let signer_seeds = &[
            PREFIX.as_bytes(),
            program_id.as_ref(),
            store_info.key.as_ref(),
            INDEX.as_bytes(),
            as_string.as_bytes(),
            &[bump],
        ];

        create_or_allocate_account_raw(
            *program_id,
            store_index_info,
            rent_info,
            system_info,
```

```
            payer_info,
            MAX_STORE_INDEXER_SIZE,
            signer_seeds,
        )?;
    }

    assert_owned_by(store_index_info, program_id)?;

    let mut indexer = StoreIndexer::from_account_info(store_index_info)?;
    indexer.key = Key::StoreIndexerV1;
    indexer.store = *store_info.key;
    indexer.page = page;

    if offset_u > indexer.auction_caches.len() {
        return Err(MetaplexError::InvalidCacheOffset.into());
    }

    if indexer.auction_caches.len() > 0 && offset_u <
    ↪  indexer.auction_caches.len() - 1 {
        let above_key = &indexer.auction_caches[offset_u];
        if let Some(abo) = &above_cache {
            if let Some(above_cache_info_unwrapped) = above_cache_info {
                if above_cache_info_unwrapped.key != above_key {
                    return Err(MetaplexError::CacheMismatch.into());
                } else if abo.timestamp > auction_cache.timestamp {
                    return Err(MetaplexError::CacheAboveIsNewer.into());
                }
            } else {
                msg!("Should never happen");
                return Err(MetaplexError::InvalidOperation.into());
            }
        } else {
            return
            ↪  Err(MetaplexError::ExpectedAboveAuctionCacheToBeProvided.into());
        }
    }

    if offset_u > 0 {
        let below_key = &indexer.auction_caches[offset_u - 1];
        // special case where you're at top of stack, there is no above
        let cache_used_for_below = if offset_u ==
        ↪  indexer.auction_caches.len() - 1 {
```

```
172             &above_cache
173         } else {
174             &below_cache
175         };
176
177         let cache_info_used_for_below = if offset_u ==
            ↪ indexer.auction_caches.len() - 1 {
178             above_cache_info
179         } else {
180             below_cache_info
181         };
182
183         if let Some(bel) = cache_used_for_below {
184             if let Some(below_cache_info_unwrapped) =
                ↪ cache_info_used_for_below {
185                 if below_cache_info_unwrapped.key != below_key {
186                     return Err(MetaplexError::CacheMismatch.into());
187                 } else if bel.timestamp < auction_cache.timestamp {
188                     return Err(MetaplexError::CacheBelowIsOlder.into());
189                 }
190             } else {
191                 msg!("Should never happen");
192                 return Err(MetaplexError::InvalidOperation.into());
193             }
194         } else {
195             return
                ↪ Err(MetaplexError::ExpectedAboveAuctionCacheToBeProvided.into());
196         }
197     }
198
199     let mut new_vec = vec![];
200
201     for n in 0..offset_u {
202         new_vec.push(indexer.auction_caches[n])
203     }
204
205     new_vec.push(*auction_cache_info.key);
206
207     for n in offset_u..indexer.auction_caches.len() {
208         if new_vec.len() == MAX_INDEXED_ELEMENTS {
209             break;
210         }
```

```
211         new_vec.push(indexer.auction_caches[n])
212     }
213 
214     indexer.auction_caches = new_vec;
215     indexer.serialize(&mut *store_index_info.data.borrow_mut())?;
216     Ok(())
217 }
218 
```

- Call Stack

```
1 processor::set_store_index::process_set_store_index
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_6: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/deprecated_init_auction_manager_v1.rs:20:1: 133:2

```
20 pub fn process_deprecated_init_auction_manager_v1(
21     program_id: &Pubkey,
22     accounts: &[AccountInfo],
23     auction_manager_settings: AuctionManagerSettingsV1,
24 ) -> ProgramResult {
25     let account_info_iter = &mut accounts.iter();
26 
27     let auction_manager_info = next_account_info(account_info_iter)?;
28     let vault_info = next_account_info(account_info_iter)?;
29     let auction_info = next_account_info(account_info_iter)?;
30     let authority_info = next_account_info(account_info_iter)?;
31     let payer_info = next_account_info(account_info_iter)?;
32     let accept_payment_info = next_account_info(account_info_iter)?;
33     let store_info = next_account_info(account_info_iter)?;
34     let system_info = next_account_info(account_info_iter)?;
35     let rent_info = next_account_info(account_info_iter)?;
36     let (bump_seed, vault, auction) = assert_common_checks(
37         program_id,
38         auction_manager_info,
39         vault_info,
40         auction_info,
41         store_info,
42         accept_payment_info,
43         authority_info,
44     )?;
45 
46     if auction_manager_settings.winning_configs.len() !=
    ↪  auction.num_possible_winners() as usize {
```

```
47          return Err(MetaplexError::WinnerAmountMismatch.into());
48      }
49
50      let mut winning_config_states: Vec<WinningConfigState> = vec![];
51      let mut winning_item_count: u8 = 0;
52      let mut any_with_more_than_one = false;
53      for winning_config in &auction_manager_settings.winning_configs {
54          let mut winning_config_state_items = vec![];
55          let mut safety_deposit_box_found_lookup: Vec<bool> = vec![];
56          for _ in 0..vault.token_type_count {
57              safety_deposit_box_found_lookup.push(false)
58          }
59          if winning_config.items.len() > 1 {
60              any_with_more_than_one = true;
61          }
62          for item in &winning_config.items {
63              // If this blows then they have more than 255 total items which
                ↪  is unacceptable in current impl
64              winning_item_count = winning_item_count
65                  .checked_add(1)
66                  .ok_or(MetaplexError::NumericalOverflowError)?;
67
68              // Check if index referenced exists
69              if item.safety_deposit_box_index as usize >=
                ↪  safety_deposit_box_found_lookup.len() {
70                  return
                    ↪  Err(MetaplexError::InvalidWinningConfigSafetyDepositIndex.into());
71              }
72
73              // Should never have same deposit index appear twice in one
                ↪  config.
74              let lookup =
                ↪  safety_deposit_box_found_lookup[item.safety_deposit_box_index
                ↪  as usize];
75              if lookup {
76                  return
                    ↪  Err(MetaplexError::DuplicateWinningConfigItemDetected.into());
77              } else {
78
↪   safety_deposit_box_found_lookup[item.safety_deposit_box_index as usize]
↪   = true
79              }
```

```
80
81              if item.safety_deposit_box_index > vault.token_type_count {
82                  return Err(MetaplexError::InvalidSafetyDepositBox.into());
83              }
84
85              winning_config_state_items.push(WinningConfigStateItem {
86                  claimed: false,
87                  primary_sale_happened: false,
88              })
89          }
90          winning_config_states.push(WinningConfigState {
91              items: winning_config_state_items,
92              money_pushed_to_accept_payment: false,
93          })
94      }
95
96      let authority_seeds = &[PREFIX.as_bytes(), &auction_info.key.as_ref(),
        ↪  &[bump_seed]];
97
98      create_or_allocate_account_raw(
99          *program_id,
100         auction_manager_info,
101         rent_info,
102         system_info,
103         payer_info,
104         MAX_AUCTION_MANAGER_V1_SIZE,
105         authority_seeds,
106     )?;
107
108     let mut auction_manager =
        ↪  AuctionManagerV1::from_account_info(auction_manager_info)?;
109
110     auction_manager.key = Key::AuctionManagerV1;
111     auction_manager.store = *store_info.key;
112     auction_manager.state.status = AuctionManagerStatus::Initialized;
113     auction_manager.settings = auction_manager_settings;
114     auction_manager.vault = *vault_info.key;
115     auction_manager.auction = *auction_info.key;
116     auction_manager.authority = *authority_info.key;
117     auction_manager.accept_payment = *accept_payment_info.key;
118     auction_manager.state.winning_config_items_validated = 0;
119     auction_manager.state.winning_config_states = winning_config_states;
```

```
    auction_manager.straight_shot_optimization = !any_with_more_than_one;

    if auction_manager.settings.participation_config.is_some() {
        auction_manager.state.participation_state =
↪   Some(ParticipationStateV1 {
            collected_to_accept_payment: 0,
            validated: false,
            primary_sale_happened: false,
            printing_authorization_token_account: None,
        })
    }
    auction_manager.serialize(&mut
↪   *auction_manager_info.data.borrow_mut())?;

    Ok(())
}

```

- Call Stack

```
processor::deprecated_init_auction_manager_v1::process_deprecated_init_auction_manager_v
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_7: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

`Todo: Add owner variable`

- Location

metaplex/program/src/processor/init_auction_manager_v2.rs:97:1: 196:2

```
97  pub fn process_init_auction_manager_v2(
98      program_id: &Pubkey,
99      accounts: &[AccountInfo],
100     amount_type: TupleNumericType,
101     length_type: TupleNumericType,
102     max_ranges: u64,
103 ) -> ProgramResult {
104     let account_info_iter = &mut accounts.iter();
105 
106     let auction_manager_info = next_account_info(account_info_iter)?;
107     let auction_token_tracker_info = next_account_info(account_info_iter)?;
108     let vault_info = next_account_info(account_info_iter)?;
109     let auction_info = next_account_info(account_info_iter)?;
110     let authority_info = next_account_info(account_info_iter)?;
111     let payer_info = next_account_info(account_info_iter)?;
112     let accept_payment_info = next_account_info(account_info_iter)?;
113     let store_info = next_account_info(account_info_iter)?;
114     let system_info = next_account_info(account_info_iter)?;
115     let rent_info = next_account_info(account_info_iter)?;
116 
117     let (bump_seed, _vault, _auction) = assert_common_checks(
118         program_id,
119         auction_manager_info,
120         vault_info,
121         auction_info,
122         store_info,
123         accept_payment_info,
124         authority_info,
```

```
125     )?;
126
127     let authority_seeds = &[PREFIX.as_bytes(), &auction_info.key.as_ref(),
        ↪  &[bump_seed]];
128
129     create_or_allocate_account_raw(
130         *program_id,
131         auction_manager_info,
132         rent_info,
133         system_info,
134         payer_info,
135         MAX_AUCTION_MANAGER_V2_SIZE,
136         authority_seeds,
137     )?;
138
139     let mut auction_manager =
        ↪  AuctionManagerV2::from_account_info(auction_manager_info)?;
140
141     auction_manager.key = Key::AuctionManagerV2;
142     auction_manager.store = *store_info.key;
143     auction_manager.state.status = AuctionManagerStatus::Initialized;
144     auction_manager.vault = *vault_info.key;
145     auction_manager.auction = *auction_info.key;
146     auction_manager.authority = *authority_info.key;
147     auction_manager.accept_payment = *accept_payment_info.key;
148     auction_manager.state.safety_config_items_validated = 0;
149     auction_manager.state.bids_pushed_to_accept_payment = 0;
150
151     auction_manager.serialize(&mut
↪   *auction_manager_info.data.borrow_mut())?;
152
153     if !auction_token_tracker_info.data_is_empty() {
154         return Err(ProgramError::AccountAlreadyInitialized);
155     } else {
156         let token_bump = assert_derivation(
157             program_id,
158             auction_token_tracker_info,
159             &[
160                 PREFIX.as_bytes(),
161                 &program_id.as_ref(),
162                 auction_manager_info.key.as_ref(),
163                 TOTALS.as_bytes(),
```

```
            ],
        )?;

        let token_type_tracker = AuctionWinnerTokenTypeTracker {
            key: Key::AuctionWinnerTokenTypeTrackerV1,
            amount_type,
            length_type,
            amount_ranges: vec![],
        };

        let token_seeds = &[
            PREFIX.as_bytes(),
            &program_id.as_ref(),
            auction_manager_info.key.as_ref(),
            TOTALS.as_bytes(),
            &[token_bump],
        ];

        create_or_allocate_account_raw(
            *program_id,
            auction_token_tracker_info,
            rent_info,
            system_info,
            payer_info,
            token_type_tracker.created_size(max_ranges),
            token_seeds,
        )?;

        token_type_tracker.save(&auction_token_tracker_info);
    }

    Ok(())
}

```

- Call Stack

```
processor::init_auction_manager_v2::process_init_auction_manager_v2
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_8: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/set_auction_cache.rs:19:1: 143:2

```
19 pub fn process_set_auction_cache<'a>(
20     program_id: &'a Pubkey,
21     accounts: &'a [AccountInfo<'a>],
22 ) -> ProgramResult {
23     let account_info_iter = &mut accounts.iter();
24 
25     let auction_cache_info = next_account_info(account_info_iter)?;
26     let payer_info = next_account_info(account_info_iter)?;
27     let auction_info = next_account_info(account_info_iter)?;
28     let safety_deposit_box_info = next_account_info(account_info_iter)?;
29     let auction_manager_info = next_account_info(account_info_iter)?;
30     let store_info = next_account_info(account_info_iter)?;
31     let system_info = next_account_info(account_info_iter)?;
32     let rent_info = next_account_info(account_info_iter)?;
33     let clock_info = next_account_info(account_info_iter)?;
34     let clock = Clock::from_account_info(clock_info)?;
35     let store = Store::from_account_info(store_info)?;
36     let _auction = AuctionData::from_account_info(auction_info)?;
37     let auction_manager =
       ↪ AuctionManagerV2::from_account_info(auction_manager_info)?;
38     let deposit_box =
       ↪ SafetyDepositBox::from_account_info(safety_deposit_box_info)?;
39 
40     assert_signer(payer_info)?;
41 
42     assert_owned_by(store_info, program_id)?;
43     assert_owned_by(auction_manager_info, program_id)?;
44     assert_owned_by(auction_info, &store.auction_program)?;
```

```
45      assert_owned_by(safety_deposit_box_info, &store.token_vault_program)?;
46
47      assert_derivation(
48          &store.auction_program,
49          auction_info,
50          &[
51              mpl_auction::PREFIX.as_bytes(),
52              store.auction_program.as_ref(),
53              deposit_box.vault.as_ref(),
54          ],
55      )?;
56
57      assert_derivation(
58          &store.token_vault_program,
59          safety_deposit_box_info,
60          &[
61              mpl_token_vault::state::PREFIX.as_bytes(),
62              auction_manager.vault.as_ref(),
63              deposit_box.token_mint.as_ref(),
64          ],
65      )?;
66
67      if deposit_box.vault != auction_manager.vault {
68          return Err(MetaplexError::InvalidSafetyDepositBox.into());
69      }
70
71      if system_info.key != &solana_program::system_program::id() {
72          return Err(MetaplexError::InvalidSystemProgram.into());
73      }
74
75      let bump = assert_derivation(
76          program_id,
77          auction_cache_info,
78          &[
79              PREFIX.as_bytes(),
80              program_id.as_ref(),
81              store_info.key.as_ref(),
82              auction_info.key.as_ref(),
83              CACHE.as_bytes(),
84          ],
85      )?;
86
```

```
87      let (metadata, _) = Pubkey::find_program_address(
88          &[
89              mpl_token_metadata::state::PREFIX.as_bytes(),
90              store.token_metadata_program.as_ref(),
91              deposit_box.token_mint.as_ref(),
92          ],
93          &store.token_metadata_program,
94      );
95
96      let mut cache: AuctionCache;
97      if auction_cache_info.data_is_empty() {
98          let signer_seeds = &[
99              PREFIX.as_bytes(),
100             program_id.as_ref(),
101             store_info.key.as_ref(),
102             auction_info.key.as_ref(),
103             CACHE.as_bytes(),
104             &[bump],
105         ];
106
107         create_or_allocate_account_raw(
108             *program_id,
109             auction_cache_info,
110             rent_info,
111             system_info,
112             payer_info,
113             MAX_AUCTION_CACHE_SIZE,
114             signer_seeds,
115         )?;
116         cache = AuctionCache::from_account_info(auction_cache_info)?;
117         cache.timestamp = clock.unix_timestamp;
118         cache.store = *store_info.key;
119     } else {
120         cache = AuctionCache::from_account_info(auction_cache_info)?;
121     }
122
123     assert_owned_by(auction_cache_info, program_id)?;
124
125     cache.key = Key::AuctionCacheV1;
126     cache.vault = auction_manager.vault;
127     cache.auction_manager = *auction_manager_info.key;
128     cache.auction = *auction_info.key;
```

```
129
130     if cache.metadata.len() == MAX_METADATA_PER_CACHE {
131         return Err(MetaplexError::MaxMetadataCacheSizeReached.into());
132     }
133     for key in &cache.metadata {
134         if key == &metadata {
135             return Err(MetaplexError::DuplicateKeyDetected.into());
136         }
137     }
138
139     cache.metadata.push(metadata);
140     cache.serialize(&mut *auction_cache_info.data.borrow_mut())?;
141
142     Ok(())
143 }
144
```

- Call Stack

```
1 processor::set_auction_cache::process_set_auction_cache
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: CHK_CVE_9: MissingCheckerCve - is_owner

Category	Severity	Status
Missing Owner Check	Critical	UnResolved

- Variable

Todo: Add owner variable

- Location

metaplex/program/src/processor/set_store.rs:122:1: 193:2

```
122 pub fn process_set_store_v2<'a>(
123     program_id: &'a Pubkey,
124     accounts: &'a [AccountInfo<'a>],
125     public: bool,
126     settings_uri: Option<String>,
127 ) -> ProgramResult {
128     let account_info_iter = &mut accounts.iter();
129 
130     let store_info = next_account_info(account_info_iter)?;
131     let store_config_info = next_account_info(account_info_iter)?;
132     let admin_wallet_info = next_account_info(account_info_iter)?;
133     let payer_info = next_account_info(account_info_iter)?;
134     let token_program_info = next_account_info(account_info_iter)?;
135     let token_vault_program_info = next_account_info(account_info_iter)?;
136     let token_metadata_program_info =
        ↪  next_account_info(account_info_iter)?;
137     let auction_program_info = next_account_info(account_info_iter)?;
138     let system_info = next_account_info(account_info_iter)?;
139     let rent_info = next_account_info(account_info_iter)?;
140 
141     let res = set_store_logic(
142         public,
143         program_id,
144         auction_program_info,
145         token_vault_program_info,
146         rent_info,
147         system_info,
148         token_metadata_program_info,
```

```
        token_program_info,
        store_info,
        admin_wallet_info,
        payer_info,
    );
    if res.is_err() {
        return res;
    }
    if !store_config_info.data_is_empty() {
        assert_owned_by(store_config_info, program_id)?;
    }
    let store_config_bump = assert_derivation(
        program_id,
        store_config_info,
        &[
            PREFIX.as_bytes(),
            program_id.as_ref(),
            CONFIG.as_bytes(),
            store_info.key.as_ref(),
        ],
    )?;

    if store_config_info.data_is_empty() {
        create_or_allocate_account_raw(
            *program_id,
            store_config_info,
            rent_info,
            system_info,
            payer_info,
            MAX_STORE_CONFIG_V1_SIZE,
            &[
                PREFIX.as_bytes(),
                program_id.as_ref(),
                CONFIG.as_bytes(),
                store_info.key.as_ref(),
                &[store_config_bump],
            ],
        )?;
    }
    let mut config = StoreConfig::from_account_info(store_config_info)?;
    config.key = Key::StoreConfigV1;
    config.settings_uri = settings_uri;
```

```
191     config.serialize(&mut *store_config_info.data.borrow_mut())?;
192     Ok(())
193 }
194
```

- Call Stack

```
1 processor::set_store::process_set_store_v2
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

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.