

Assure DeFi[®]

THE VERIFICATION **GOLD STANDARD**



Security Assessment

GameDay

Date: 21/08/2024

Audit Status: PASS

Audit Edition: Advanced



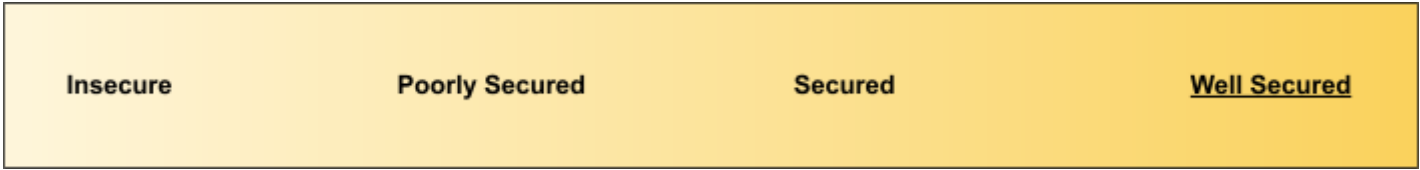
Risk Analysis

Vulnerability summary

Classification	Description
 High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
 Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
 Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
 Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Well Secured**.



Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the GameDay contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

Target Code And Revision

Project	Assure
Language	Solidity
Codebase	GameDayToken.zip - [SHA256] 8c8af57b4b6acc8e623175bcc1e6af98b61e5851301c0c8c4425b6450feb2a35
Audit Methodology	Static, Manual

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	<ul style="list-style-type: none">• Compiler warnings.• Race conditions and Reentrancy. Cross-function race conditions.• Possible delays in data delivery.• Oracle calls.• Front running.• Timestamp dependence.• Integer Overflow and Underflow.• DoS with Revert.• DoS with block gas limit.• Methods execution permissions.• Economy model.• Private user data leaks.• Malicious Event log.• Scoping and Declarations.• Uninitialized storage pointers.• Arithmetic accuracy.• Design Logic.• Cross-function race conditions.• Safe Zeppelin module.• Fallback function security.• Overpowered functions / Owner privileges

AUDIT OVERVIEW



No high severity issues were found.



No medium severity issues were found.



No low severity issues were found.



No Informational severity issues were found.

Testing coverage

During the testing phase, custom use cases were written to cover all the logic of contracts. *Check “Annexes” to see the testing code.

GameDay contracts tests:

tests/test_game_day_token.py::test_mint_burn **RUNNING**

Transaction sent: **0xbcb8120adf73d5b186ce0e8580dd76a492d0160184a1054a3b300d0f467b4b37**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **0**

Access.constructor confirmed Block: **1** Gas used: **1119055 (9.33%)**

Access deployed at: **0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87**

Transaction sent: **0xbc9da3b535c39ee194d1e83cf711421a3b45aa6a8e5ec783a232c5b69d2757d9**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **1**

SystemPause.constructor confirmed Block: **2** Gas used: **2017102 (16.81%)**

SystemPause deployed at: **0x602C71e4DAC47a042Ee7f46E0aee17F94A3bA0B6**

Transaction sent: **0x87efb2406a31f84c7fe5c31c2c7551ad1266730aca18abdbf944cc1d66ddcb06**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **2**

GameDayToken.constructor confirmed Block: **3** Gas used: **2587268 (21.56%)**

GameDayToken deployed at: **0xE7eD6747FaC5360f88a2EFC03E00d25789F69291**

Transaction sent: **0x7ff5974322f7713cb1f71004a1f82ce7a5055763b6e1949ac364c9286503adb1**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **3**

GameDayToken.initialize confirmed (**Address zero input**) Block: **4** Gas used: **140921 (1.17%)**

Transaction sent: **0x29f7009927e9cb727d42eb04d84b4099cbc926dfad6fde9eb4e5822002e40d48**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **4**

GameDayToken.initialize confirmed (**Address zero input**) Block: **5** Gas used: **140950 (1.17%)**

Transaction sent: **0x96d3f094801aebcc8392b9037ce0f6ad299734bb9938bf53acbe7bd2484f8acd**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **5**

GameDayToken.initialize confirmed Block: **6** Gas used: **205526 (1.71%)**

Transaction sent: **0xd352ffc73948c1529256a65305e742abd32379e66c65449fa3182ee483f8f31a**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **6**

GameDayToken.mint confirmed (**VEXT: access forbidden**) Block: **7** Gas used: **28693 (0.24%)**

Transaction sent: **0x37b210fa73a9224c9a3b5ce0f68c8675621140f6bcd1b1da34590f249af23e28**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **7**

Access.initialize confirmed Block: **8** Gas used: **172624 (1.44%)**

Transaction sent: **0xadf45a493280b329d642af35e54700061f004a8bffffb9121d810c14a6bfa0160**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **8**

GameDayToken.mint confirmed Block: **9** Gas used: **143161 (1.19%)**

Transaction sent: **0x2c313d3180598b458256ddd622f4f9df097ba10d4dac89d5650e2d3b07a4ee4c**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **0**

GameDayToken.pauseContract confirmed (**VEXT: access forbidden**) Block: **10** Gas used: **26292 (0.22%)**

Transaction sent: **0x708c58d3d7d12716a76f3e4e9611c2583a1b2fc33144c9804ace25db890c5ca2**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **9**

GameDayToken.pauseContract confirmed Block: **11** Gas used: **48955 (0.41%)**

Transaction sent: **0xa204e198fd796f9d470bf653b750396be546f3c2792ca448a543c6e9857a0e28**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **10**

GameDayToken.mint confirmed (**Pausable: paused**) Block: **12** Gas used: **22977 (0.19%)**

Transaction sent: **0x1ff11a89d3424b7e901dfa1d3c953d37e27a939cafbe4a6c15df39112f489e9d**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **1**

GameDayToken.unpauseContract confirmed (**VEXT: access forbidden**) Block: **13** Gas used: **26269 (0.22%)**

Transaction sent: **0xd4bc58717a63c513968ae81950f3cdf8170bb80a65e17c74680dad498e519722**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **11**

GameDayToken.unpauseContract confirmed Block: **14** Gas used: **18920 (0.16%)**

Transaction sent: **0x25d7219ef0f4ed0bc6e3121da81a894a7fd715dbc71853e984288be2cc99d8ef**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **0**

GameDayToken.burn confirmed (**User can only burn owned tokens**) Block: **15** Gas used: **23889 (0.20%)**

Transaction sent: **0x6a87a27541ef7728b35e6f7fcb28a35f4828317852f24f3e1896c11696438dc6**

Gas price: **0.0** gwei Gas limit: **12000000** Nonce: **2**

GameDayToken.burn confirmed Block: **16** Gas used: **70928 (0.59%)**

tests/test_game_day_token.py::test_mint_burn **PASSED**

```
tests/test_game_day_token.py::test_transfer RUNNING  
Transaction sent: 0xa3272e284fed53739d0b768418f5de02476d9fa6eaa208d2af9bfd6c7442f4a0  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 12  
Access.constructor confirmed Block: 17 Gas used: 1119055 (9.33%)  
Access deployed at: 0x2c15A315610Bfa5248E4CbCbd693320e9D8E03Cc  
  
Transaction sent: 0x40bcbf1643c9f0499228ecdc743f5e7c18119aa29343520c0f135ff0d05ea718  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 13  
SystemPause.constructor confirmed Block: 18 Gas used: 2017102 (16.81%)  
SystemPause deployed at: 0xe692Cf21B12e0B2717C4bF647F9768Fa58861c8b  
  
Transaction sent: 0x00d56a0868a748a9c42edccb9f590dab7458e69526ecd8570bd1e489292d13cb  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 14  
GameDayToken.constructor confirmed Block: 19 Gas used: 2587268 (21.56%)  
GameDayToken deployed at: 0xe65A7a341978d59d40d30FC23F5014FACB4f575A  
  
Transaction sent: 0xdd454b9196de2f89ba01345702751c17c7eadcc64c3ed9a27073337dabccd646  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 15  
GameDayToken.initialize confirmed Block: 20 Gas used: 205526 (1.71%)  
  
Transaction sent: 0x7818a6f4adf227052917c64460565701d5cdeca99db4cf3050b2ee986298e8db  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 16  
Access.initialize confirmed Block: 21 Gas used: 172624 (1.44%)  
  
Transaction sent: 0xa6d5ca4c5c64dcfac68e1c5bdd000a80fd08c522bcf498b3c29d0da776512813  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 17  
GameDayToken.mint confirmed Block: 22 Gas used: 143161 (1.19%)  
  
Transaction sent: 0xd19032803cf16bdfb1b8daf3ca0407a2e00caab264f2e320ad2c7e2029734dda  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 3  
GameDayToken.transfer confirmed Block: 23 Gas used: 64775 (0.54%)  
  
Transaction sent: 0x59f0a39d65487b47227a253d20043ae4611c18713e581f85fec85dde492cc383  
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 1  
GameDayToken.transfer confirmed Block: 24 Gas used: 64787 (0.54%)  
  
tests/test_game_day_token.py::test_transfer PASSED  
tests/test_game_day_token.py::test_mint RUNNING
```


Annexes

Testing code:

Testing_GameDay:

```
from brownie import (

    reverts,

)

from scripts.helpful_scripts import (

    ZERO_ADDRESS,

    DAY_TIMESTAMP,

    get_account,

    get_timestamp,

    get_chain_number,

    increase_timestamp

)

from scripts.deploy import (

    deploy_access,

    deploy_system_pause,

    deploy_game_day_token

)

def test_mint_burn(only_local):

    # Arrange

    owner = get_account(0)

    other = get_account(1)

    extra = get_account(2)
```

```

access = deploy_access(owner)

system_pause = deploy_system_pause(owner, access.address)

gameday_token = deploy_game_day_token(owner)


with reverts("Address zero input"):
    gameday_token.initialize(ZERO_ADDRESS, system_pause.address, 100e18, {"from":
owner})

with reverts("Address zero input"):
    gameday_token.initialize(access.address, ZERO_ADDRESS, 100e18, {"from": owner})

gameday_token.initialize(access.address, system_pause, 1000e18, {"from": owner})

with reverts("VEXT: access forbidden"):
    gameday_token.mint(other, 10e18, {"from": owner})

access.initialize(owner, owner, owner, {"from": owner})


tx = gameday_token.mint(other, 10e18, {"from": owner})

assert tx.events['Transfer'][0]['from'] == ZERO_ADDRESS
assert tx.events['Transfer'][0]['to'] == other
assert tx.events['Transfer'][0]['value'] == 10e18


with reverts("VEXT: access forbidden"):
    gameday_token.pauseContract({"from": other})

gameday_token.pauseContract({"from": owner})


with reverts(""):
    gameday_token.mint(other, 10e18, {"from": owner})

with reverts("VEXT: access forbidden"):
    gameday_token.unpauseContract({"from": other})

```

```
gameday_token.unpauseContract({"from": owner})
```

```
with reverts("User can only burn owned tokens"):
```

```
    gameday_token.burn(other, 1e18, {"from": extra})
```

```
tx = gameday_token.burn(other, 1e18, {"from": other})
```

```
assert tx.events['Transfer'][0]['from'] == other
```

```
assert tx.events['Transfer'][0]['to'] == ZERO_ADDRESS
```

```
assert tx.events['Transfer'][0]['value'] == 1e18
```

```
def test_transfer(only_local):
```

```
    # Arrange
```

```
    owner = get_account(0)
```

```
    other = get_account(1)
```

```
    extra = get_account(2)
```

```
    another = get_account(3)
```

```
    access = deploy_access(owner)
```

```
    system_pause = deploy_system_pause(owner, access.address)
```

```
    gameday_token = deploy_game_day_token(owner)
```

```
    gameday_token.initialize(access.address, system_pause, 1000e18, {"from": owner})
```

```
    access.initialize(owner, owner, owner, {"from": owner})
```

```
    # mint some tokens
```

```
    gameday_token.mint(other, 10e18, {"from": owner})
```

```
    tx = gameday_token.transfer(extra, 2e18, {"from": other})
```

```
    assert tx.events['Transfer'][0]['from'] == other
```

```
    assert tx.events['Transfer'][0]['to'] == extra
```

```
    assert tx.events['Transfer'][0]['value'] == 2e18
```

```
tx = gameday_token.transfer(another, 1e18, {"from": extra})

assert tx.events['Transfer'][0]['from'] == extra

assert tx.events['Transfer'][0]['to'] == another

assert tx.events['Transfer'][0]['value'] == 1e18
```

Technical Findings Summary

Findings

Vulnerability Level	Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
<div><div></div>High</div>	0					
<div><div></div>Medium</div>	0					
<div><div></div>Low</div>	0					
<div><div></div>Informational</div>	0					

Assessment Results

Score Results

Review	Score
Global Score	90/100
Assure KYC	Pending
Audit Score	90/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS

Following our comprehensive security audit of the token contract for the GameDay project, we inform you that the project has met the necessary security standards.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.