CONTRACT WOLF

Security Assessment

FUST Staking V2

Verified on 11/18/25

SUMMARY

Project	CHAIN	METHODOLOGY
FUST	-	Manual & Automatic Analysis

FILES	DELIVERY	TYPE
Single	11/18/25	Standard Audit

4	0	0	0	2	2	4
Total Findings	Critical	Major	Medium	Minor	Informational	Resolved

🟥 0 Critical	An exposure that can affect the contract functions in several events that can risk and disrupt the contract
🟧 0 Major	An opening & exposure to manipulate the contract in an unwanted manner
🟧 0 Medium	An opening that could affect the outcome in executing the contract in a specific situation
⬜ 2 Minor	An opening but doesn't have an impact on the functionality of the contract
🟦 2 Informational	An opening that consists information but will not risk or affect the contract
🟩 4 Resolved	ContractWolf's findings has been acknowledged & resolved by the project

STATUS ✔️**AUDIT PASSED**

TABLE OF CONTENTS | FUST Staking

DISCLAIMER | FUST Staking

ContractWolf audits and reports should not be considered as a form of project's "Advertisement" and does not cover any interaction and assessment from "Project Contract" to "External Contracts" such as PancakeSwap, UniSwap, SushiSwap or similar.

ContractWolf does not provide any warranty on its released report and should not be used as a decision to invest into audited projects.

ContractWolf provides a transparent report to all its "Clients" and to its "Clients Participants" and will not claim any guarantee of bug-free code within its **SMART CONTRACT**.

ContractWolf's presence is to analyze, audit and assess the Client's Smart Contract to find any underlying risk and to eliminate any logic and flow errors within its code.

Each company or project should be liable to its security flaws and functionalities.

SCOPE OF WORK | FUST Staking

FUST's team has agreed and provided us with the files that need to be tested (*Github, BSCscan, Etherscan, Local files etc*). The scope of audit is the main contract.

The goal of this engagement is to identify if there is a possibility of security flaws in the implementation of smart contract and its systems.

ContractWolf will be focusing on contract issues and functionalities along with the project claims from smart contract to their website, whitepaper, repository which has been provided by **FUST**.

AUDITING APPROACH | FUST Staking

Every line of code along with its functionalities will undergo manual review to check for security issues, quality of logic and contract scope of inheritance. The manual review will be done by our team that will document any issues that they discovered.

METHODOLOGY

The auditing process follows a routine series of steps :

1. Code review that includes the following :
   - Review of the specifications, sources and instructions provided to ContractWolf to make sure we understand the size, scope and functionality of the smart contract.
   - Manual review of code. Our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities, underlying and hidden security flaws.

2. Testing and automated analysis that includes :
   - Testing the smart contract function with common test cases and scenarios to ensure that it returns the expected results.

3. Best practices and ethical review. The team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security and control within the smart contract.

4. Recommendations to help the project take steps to eliminate or minimize threats and secure the smart contract.

TOKEN DETAILS | FUST Staking

FUST is a utility token with standard tokenomics which is part of the FUSD ecosystem. FUSD is an appreciating stable token due to launch in the next few weeks and FUST will be used to mine free FUSD using a staking protocol we are calling the Fusion Miner.

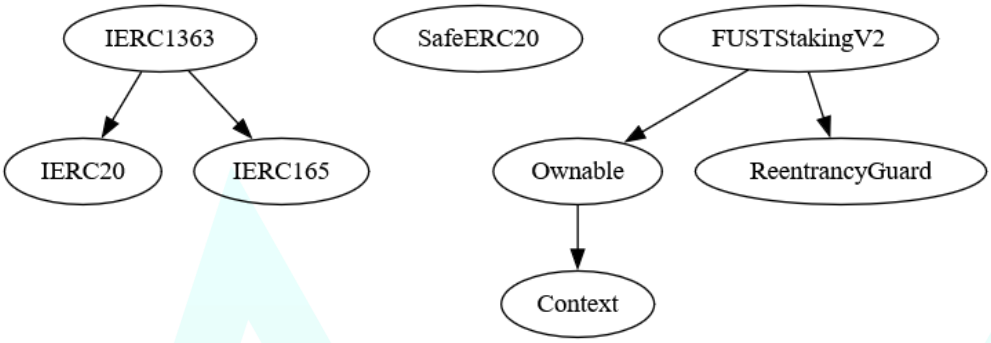
Token Name	Symbol	Decimal	Total Supply	Chain
-	-	-	-	-

SOURCE

Source	-

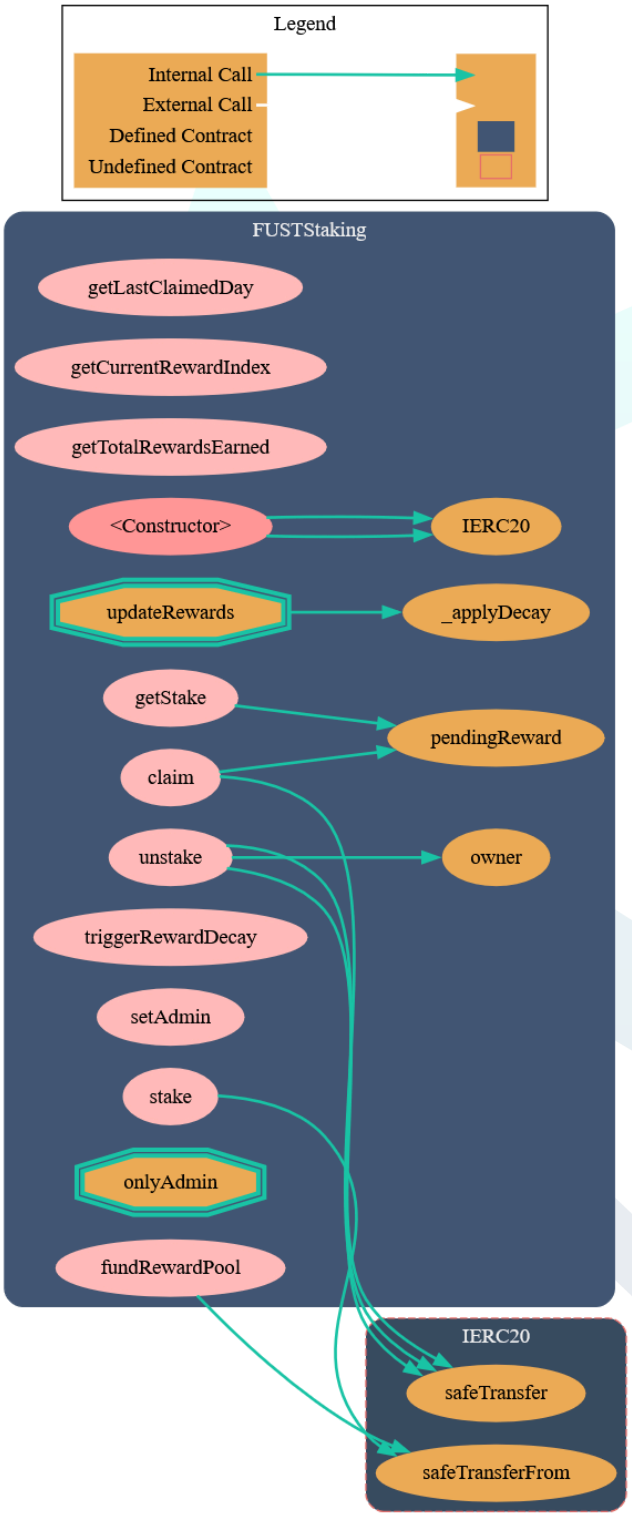
INHERITANCE GRAPH | FUST Staking

Inheritance Graph of Contract Functions



CALL GRAPH | FUST Staking

Call Graph of Contract Functions



FINDINGS | FUST Staking

Total Findings	Critical	Major	Medium	Minor	Informational	Resolved
4	0	0	0	2	2	4

This report has been prepared to state the issues and vulnerabilities for FUST Staking through this audit. The goal of this report findings is to identify specifically and fix any underlying issues and errors

ID	Title	File & Line #	Severity	Status
SWC-135	Incorrect Reward Accounting	FUSTStakingV2.sol L : 125	Minor	Resolved
SWC-123	Incorrect Unstaking Logic	FUSTStakingV2.sol L : 181	Minor	Resolved
SWC-129	Incorrect Reward Distribution Logic	FUSTStakingV2.sol L : 94	Informational	Resolved
SWC-101	Integer Overflow/underflow	FUSTStakingV2.sol L : 89	Informational	Resolved

SWC ATTACKS | FUST Staking

Smart Contract Weakness Classification and Test Cases

ID	Description	Status
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELF DESTRUCT Instruction	Passed
SWC-107	Reentrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed

ID	Description	Status
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character(U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

CW ASSESSMENT | FUST Staking

ContractWolf Vulnerability and Security Tests

ID	Name	Description	Status
CW-001	Multiple Version	Presence of multiple compiler version across all contracts	✔
CW-002	Incorrect Access Control	Additional checks for critical logic and flow	✔
CW-003	Payable Contract	A function to withdraw ether should exist otherwise the ether will be trapped	✔
CW-004	Custom Modifier	major recheck for custom modifier logic	✔
CW-005	Divide Before Multiply	Performing multiplication before division is generally better to avoid loss of precision	✔
CW-006	Multiple Calls	Functions with multiple internal calls	✔
CW-007	Deprecated Keywords	Use of deprecated functions/operators such as block.blockhash() for blockhash(), msg.gas for gasleft(), throw for revert(), sha3() for keccak256(), callcode() for delegatecall(), suicide() for selfdestruct(), constant for view or var for actual type name should be avoided to prevent unintended errors with newer compiler versions	✔
CW-008	Unused Contract	Presence of an unused, unimported or uncalled contract	✔
CW-009	Assembly Usage	Use of EVM assembly is error-prone and should be avoided or double-checked for correctness	✔
CW-010	Similar Variable Names	Variables with similar names could be confused for each other and therefore should be avoided	✔
CW-011	Commented Code	Removal of commented/unused code lines	✔
CW-012	SafeMath Override	SafeMath is no longer needed starting with Solidity v0.8+. The compiler now has built-in overflow checking.	✔

FIXES & RECOMMENDATION

SWC-101 | Integer overflow/underflow

Potential division by zero in **`_applyDecay`** function.

```
accRewardPerShare += (dailyReward * 1e18) / totalStaked;
```

Recommendation

If **`totalStaked`** becomes zero during the loop (due to all users unstaking), this will cause division by zero.

```
// Only update accRewardPerShare if there are staked tokens
if (totalStaked > 0) {
    accRewardPerShare += (dailyReward * 1e18) / totalStaked;
}
```

SWC-123 | Incorrect Unstaking Logic

The **unstake** function doesn't properly handle the **stake** array, This leaves empty slots in the array, wasting gas and causing issues.

```
data.amount = 0; // Just sets amount to zero, doesn't remove from array
```

Recommendation

Implement proper array management

```
//data.amount = 0; //delete this and replace with a removal from stake logic
    // Remove from array by swapping with last element
    if (index != userStakes.length - 1) {
        userStakes[index] = userStakes[userStakes.length - 1];
    }
    userStakes.pop();
```

SWC-129 | Incorrect Reward Distribution Logic

The reward decay mechanism doesn't account for actual time passed properly in **_applyDecay**, This can skip partial days and doesn't handle the remainder time.

```
lastUpdate += daysElapsed * 1 days; // INCORRECT TIME UPDATE
```

Recommendation

```
function _applyDecay() internal {
    if (rewardPool == 0) {
        lastUpdate = block.timestamp;
        return;
    }

    uint256 timeElapsed = block.timestamp - lastUpdate;
    if (timeElapsed == 0) return;

    // Calculate rewards based on actual time elapsed, not just full days
    uint256 rewardPerSecond = (rewardPool * DAILY_REWARD_PERCENT) / PRECISION / 1 days;
    uint256 totalReward = rewardPerSecond * timeElapsed;

    if (totalReward > rewardPool) {
        totalReward = rewardPool;
    }

    rewardPool -= totalReward;

    if (totalStaked > 0) {
        accRewardPerShare += (totalReward * 1e18) / totalStaked;
    }

    lastUpdate = block.timestamp;
}
```

SWC-135 | Incorrect Reward Accounting

Reward calculation can overflow or underflow due to improper precision handling in **`pendingReward`**

Recommendation

If **`accRewardPerShare`** is less than **`rewardDebt`** (can happen with reward adjustments), this will underflow.

```
function pendingReward(address account) public view returns (uint256) {
    StakeData[] memory userStakes = stakes[account];
    uint256 total;
    for (uint256 i = 0; i < userStakes.length; i++) {
        if (userStakes[i].amount > 0) {
            if (accRewardPerShare > userStakes[i].rewardDebt) {
                total += (userStakes[i].amount * (accRewardPerShare -
userStakes[i].rewardDebt)) / 1e18;
            }
        }
    }
    return total;
}
```

AUDIT COMMENTS | FUST Staking

Smart Contract audit comment for a non-technical perspective

- 🟢 Contract does not have taxes
- 🟢 Contract cannot be paused
- 🟢 Owner can transfer ownership
- 🟢 Owner cannot set max transaction limit
- 🟢 Owner cannot block users

CONTRACTWOLF

Blockchain Security - Smart Contract Audits