

**Smart Contract Security Audit Report** 





The SlowMist Security Team received the CTSI team's application for smart contract security audit of the DelayedWithdraw on Sep. 17, 2020. The following are the details and results of this smart contract security audit:

### Project name:

DelayedWithdraw

File name and hash(SHA256)

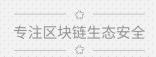
audit.zip: cb615acfc675083a89b0f3ac876f6576474d4db4fdf19b70d0b60e2555165212

### The audit items and results:

(Other unknown security vulnerabilities are not included in the audit responsibility scope)

No.	Audit Items	Audit Subclass	Audit Subclass Result
1	Overflow Audit		Passed
2	Race Conditions Audit		Passed
	Authority Control Audit	Permission vulnerability audit	Passed
3		Excessive auditing authority	Passed
	Safety Design Audit	Zeppelin module safe use	Passed
		Compiler version security	Passed
		Hard-coded address security	Passed
4		Fallback function safe use	Passed
		Show coding security	Passed
		Function return value security	Passed
		Call function security	Passed
5	Denial of Service Audit		Passed
6	Gas Optimization Audit		Passed
7	Design Logic Audit		Passed
8	"False Deposit" vulnerability Audit	30111	Passed
9	Malicious Event Log Audit		Passed
10	Scoping and Declarations Audit	-	Passed





11	Replay Attack Audit	ECDSA's Signature Replay	Passed
	Tiopiay Attack Addit	Audit	
12	Uninitialized Storage Pointers Audit		Passed
13	Arithmetic Accuracy Deviation Audit		Passed

Audit Result: Passed

Audit Number: 0X002009210001

Audit Date : Sep. 21, 2020

Audit Team: SlowMist Security Team

(Statement: SlowMist only issues this report based on the fact that has occurred or existed before the report is issued, and bears the corresponding responsibility in this regard. For the facts occur or exist later after the report, SlowMist cannot judge the security status of its smart contract. SlowMist is not responsible for it. The security audit analysis and other contents of this report are based on the documents and materials provided by the information provider to SlowMist as of the date of this report (referred to as "the provided information"). SlowMist assumes that: there has been no information missing, tampered, deleted, or concealed. If the information provided has been missed, modified, deleted, concealed or reflected and is inconsistent with the actual situation, SlowMist will not bear any responsibility for the resulting loss and adverse effects. SlowMist will not bear any responsibility for the background or other circumstances of the project.)

Summary: This is the DelayedWithdraw section of the CTSI project. OpenZeppelin's SafeMath security module is used, which is a commendable approach. The contract does not have the Overflow and the Race Conditions issue. The comprehensive evaluation contract is no risk.

The source code:

Context.sol:

//SlowMist// The contract does not have the Overflow and the Race Conditions issue

pragma solidity ^0.6.0;

/\*

- \* @dev Provides information about the current execution context, including the
- \* sender of the transaction and its data. While these are generally available
- \* via msg.sender and msg.data, they should not be accessed in such a direct
- \* manner, since when dealing with GSN meta-transactions the account sending and
- \* paying for execution may not be the actual sender (as far as an application
- \* is concerned).

\*

\* This contract is only required for intermediate, library-like contracts.

\*/



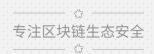


```
contract Context {
    // Empty internal constructor, to prevent people from mistakenly deploying
    // an instance of this contract, which should be used via inheritance.
    constructor () internal { }
    function _msgSender() internal view virtual returns (address payable) {
        return msg.sender;
   }
    function _msgData() internal view virtual returns (bytes memory) {
              // silence state mutability
                                                        warning without generating
                                                                                               bytecode
                                                                                                                  see
https://github.com/ethereum/solidity/issues/2691
        return msg.data;
   }
}
```

#### Ownable.sol:

```
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.6.0;
import "../GSN/Context.sol";
 * @dev Contract module which provides a basic access control mechanism, where
 * there is an account (an owner) that can be granted exclusive access to
 * specific functions.
 * By default, the owner account will be the one that deploys the contract. This
 * can later be changed with {transferOwnership}.
 * This module is used through inheritance. It will make available the modifier
 * 'onlyOwner', which can be applied to your functions to restrict their use to
 * the owner.
 */
contract Ownable is Context {
   address private _owner;
   event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);
     * @dev Initializes the contract setting the deployer as the initial owner.
```





```
*/
   constructor () internal {
        address msgSender = _msgSender();
        _owner = msgSender;
       emit OwnershipTransferred(address(0), msgSender);
   }
     * @dev Returns the address of the current owner.
   function owner() public view returns (address) {
       return _owner;
   }
     * @dev Throws it called by any account other than the owner.
   modifier onlyOwner() {
        require(_owner == _msgSender(), "Ownable: caller is not the owner");
   }
     * @dev Leaves the contract without owner. It will not be possible to call
     * 'onlyOwner' functions anymore. Can only be called by the current owner.
     * NOTE: Renouncing ownership will leave the contract without an owner,
     * thereby removing any functionality that is only available to the owner.
     */
   function renounceOwnership() public virtual onlyOwner {
        emit OwnershipTransferred(_owner, address(0));
        _owner = address(0);
   }
     * @dev Transfers ownership of the contract to a new account ('newOwner').
     * Can only be called by the current owner.
   function transferOwnership(address newOwner) public virtual onlyOwner {
        require(newOwner != address(0), "Ownable: new owner is the zero address"); //SlowMist// This check is quite
good in avoiding losing control of the contract caused by user mistakes
```



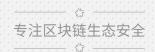


```
emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

#### IERC20.sol:

```
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.6.0;
 * @dev Interface of the ERC20 standard as defined in the EIP.
 */
interface IERC20 {
    * @dev Returns the amount of tokens in existence.
   function totalSupply() external view returns (uint256);
     * @dev Returns the amount of tokens owned by 'account'.
   function balanceOf(address account) external view returns (uint256);
    /**
     * @dev Moves 'amount' tokens from the caller's account to 'recipient'.
     * Returns a boolean value indicating whether the operation succeeded.
     * Emits a {Transfer} event.
   function transfer(address recipient, uint256 amount) external returns (bool);
     * @dev Returns the remaining number of tokens that 'spender' will be
     * allowed to spend on behalf of 'owner' through {transferFrom}. This is
     * zero by default.
     * This value changes when {approve} or {transferFrom} are called.
   function allowance(address owner, address spender) external view returns (uint256);
```





```
* @dev Sets 'amount' as the allowance of 'spender' over the caller's tokens.
 * Returns a boolean value indicating whether the operation succeeded.
 * IMPORTANT: Beware that changing an allowance with this method brings the risk
 * that someone may use both the old and the new allowance by unfortunate
 * transaction ordering. One possible solution to mitigate this race
 * condition is to first reduce the spender's allowance to 0 and set the
 * desireo value afterwards:
 * https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
 * Emits an {Approval} event.
function approve(address spender, uint256 amount) external returns (bool);
 * @dev Moves 'amount' tokens from 'sender' to 'recipient' using the
 * allowance mechanism. `amount` is then deducted from the caller's
 * allowance.
 * Returns a boolean value indicating whether the operation succeeded.
 * Emits a {Transfer} event.
function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);
 * @dev Emittea when 'value' tokens are movea from one account ('from') to
 * another ('to').
 * Note that 'value' may be zero.
event Transfer(address indexed from, address indexed to, uint256 value);
 * @dev Emitteo when the allowance of a 'spender' for an 'owner' is set by
 * a call to {approve}. 'value' is the new allowance.
event Approval(address indexed owner, address indexed spender, uint256 value);
```

}





#### SafeMath.sol:

```
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.6.0;
 * @dev Wrappers over Solidity's arithmetic operations with addea overflow
 * checks.
 * Arithmetic operations in Solidity wrap on overflow. This can easily result
 * in bugs, because programmers usually assume that an overflow raises an
 * error, which is the standard behavior in high level programming languages.
 * 'SafeMath' restores this intuition by reverting the transaction when an
 * operation overflows.
 * Using this library instead of the unchecked operations eliminates an entire
 * class of bugs, so it's recommended to use it always.
//SlowMist// OpenZeppelin's SafeMath security Module is used, which is a recommend approach
library SafeMath {
     * @dev Returns the addition of two unsigned integers, reverting on
     * overflow.
     * Counterpart to Solidity's `+' operator.
     * Requirements:
     * - Addition cannot overflow.
   function add(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a + b;
       require(c >= a, "SafeMath: addition overflow");
        return c;
   }
     * @dev Returns the subtraction of two unsigned integers, reverting on
     * overflow (when the result is negative).
```





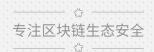
```
* Counterpart to Solidity's `-` operator.
 * Requirements:
 * - Subtraction cannot overflow.
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return sub(a, b, "SafeMath: subtraction overflow");
}
 * @dev Returns the subtraction of two unsigned integers, reverting with custom message on
 * overflow (when the result is negative).
 * Counterpart to Solidity's `-' operator.
 * Requirements:
 * - Subtraction cannot overflow.
function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
    require(b <= a, errorMessage);</pre>
    uint256 c = a - b;
    return c;
}
 * @dev Returns the multiplication of two unsigned integers, reverting on
 * overflow.
 * Counterpart to Solidity's `*` operator.
 * Requirements:
 * - Multiplication cannot overflow.
function mul(uint256 a, uint256 b) internal pure returns (uint256) {
    // Gas optimization: this is cheaper than requiring 'a not being zero, but the
    // benefit is lost it 'b is also tested.
    // See: https://github.com/OpenZeppelin/openzeppelin-contracts/pull/522
    if (a == 0) {
        return 0;
    }
```





```
uint256 c = a * b;
    require(c / a == b, "SafeMath: multiplication overflow");
    return c;
}
 * @dev Returns the integer division of two unsigned integers. Reverts on
 * division by zero. The result is rounded towards zero.
 * Counterpart to Solidity's '/' operator. Note: this function uses a
 * 'revert' opcode (which leaves remaining gas untouched) while Solidity
 * uses an invalio opcode to revert (consuming all remaining gas).
 * Requirements:
 * - The divisor cannot be zero.
function div(uint256 a, uint256 b) internal pure returns (uint256) {
    return div(a, b, "SafeMath: division by zero");
}
 * @dev Returns the integer division of two unsigned integers. Reverts with custom message on
 * division by zero. The result is rounded towards zero.
 * Counterpart to Solidity's '/' operator. Note: this function uses a
 * 'revert' opcode (which leaves remaining gas untouched) while Solidity
 * uses an invalio opcode to revert (consuming all remaining gas).
 * Requirements:
 * - The divisor cannot be zero.
function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
    // Solidity only automatically asserts when dividing by 0
    require(b > 0, errorMessage);
    uint256 c = a / b;
    // assert(a == b * c + a % b); // There is no case in which this doesn't hold
    return c;
}
/**
```





```
* @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
     * Reverts when dividing by zero.
     * Counterpart to Solidity's `%' operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalia opcode to revert (consuming all remaining gas).
     * Requirements:
     * - The divisor cannot be zero.
     */
    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        return mod(a, b, "SafeMath: modulo by zero");
    }
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
     * Reverts with custom message when dividing by zero.
     * Counterpart to Solidity's `%' operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalio opcode to revert (consuming all remaining gas).
     * Requirements:
     * - The divisor cannot be zero.
    function mod(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        require(b != 0, errorMessage);
        return a % b;
   }
}
```

### DelayedWithdraw.sol:

```
// Copyright 2020 Cartesi Pte. Ltd.

// SPDX-License-Identifier: Apache-2.0

// Licensea under the Apache License, Version 2.0 (the "License"); you may not use

// this file except in compliance with the License. You may obtain a copy of the

// License at http://www.apache.org/licenses/LICENSE-2.0

// Unless required by applicable law or agreed to in writing, software distributed

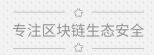
// under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
```





```
// CONDITIONS OF ANY KIND, either express or implied. See the License for the
// specific language governing permissions and limitations under the License.
/// @title DelayedWithdraw
/// @author Felipe Argento
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.6.0;
import "@openzeppelin/contracts/math/SafeMath.sol";
import "@openzeppelin/contracts/token/ERC20/IERC20.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
contract DelayedWithdraw is Ownable {
   using SafeMath for uint256;
   uint256 constant delay = 7 days;
   Withdrawal private withdrawal;
   IERC20 ctsi;
   struct Withdrawal {
        address receiver;
        uint256 amount;
        uint256 timestamp;
   }
   /// @notice Constructor
   /// @param _ctsi IERC20 that this contract is gonna work with
   constructor(IERC20 _ctsi) public {
        ctsi = _ctsi;
   }
   /// @notice Get the amount of tokens to be released next withdrawal
   function getWithdrawalAmount() public view returns (uint256) {
        return withdrawal.amount;
   }
   /// @notice Get the receiver of tokens to be released next withdrawal
   function getWithdrawalReceiver() public view returns (address) {
```





```
return withdrawal.receiver;
}
/// @notice Get the timestamp of when next withdrawai was created
function getWithdrawalTimestamp() public view returns (uint256) {
    return withdrawal.timestamp;
}
/// @notice Creates a withdrawal request that will be finalized after delay time
/// @param _receiver address that will receive the token
/// @param _amount amount of tokens for the request
function requestWithdrawal(
    address _receiver,
    uint256 _amount
)
    public
    onlyOwner()
    returns (bool)
{
    require(_amount > 0, "withdrawal amount has to be bigger than 0");
    uint256 newAmount = withdrawal.amount.add(_amount);
    require(
        newAmount <= ctsi.balanceOf(address(this)),
        "Not enough tokens in the contract for this Withdrawal request"
    );
    withdrawal.receiver = _receiver;
    withdrawal.amount = newAmount;
    withdrawal.timestamp = block.timestamp;
    emit WithdrawRequested(_receiver, newAmount, block.timestamp);
    return true;
}
/// @notice Finalizes withdraw and transfer the tokens to receiver
function finalizeWithdraw() public onlyOwner returns (bool) {
    uint256 amount = withdrawal.amount;
    require(
        withdrawal.timestamp.add(delay) <= block.timestamp,
        "Withdrawal is not old enough to be finalized"
```





```
);
        require(amount > 0, "There are no active withdrawal requests");
        withdrawal.amount = 0;
        ctsi.transfer(withdrawal.receiver, amount);
        emit WithdrawFinalized(withdrawal.receiver, amount);
        return true;
    }
    /// @notice Cancel any pending unfinalized withdrawal
    function cancelWithdrawal() public onlyOwner returns (bool) {
        require(withdrawal.amount > 0, "There are no active withdrawal requests");
        emit WithdrawCanceled(withdrawal.receiver, withdrawal.amount, block.timestamp);
        withdrawal.amount = 0;
        return true;
    }
    /// @notice Events signalling interactions
    event WithdrawRequested(address _receiver, uint256 _amount, uint256 _timestamp);
    event WithdrawCanceled(address _receiver, uint256 _amount, uint256 _timestamp);
    event WithdrawFinalized(address _receiver, uint256 _amount);
}
```



# Official Website

www.slowmist.com

# E-mail

team@slowmist.com

## **Twitter**

@SlowMist\_Team

# **WeChat Official Account**

