



JohnWick Sec

Guard the internet of value



ETH SMART CONTRACT AUDIT REPORT

JOHNWICK SECURITY LAB

WWW.JOHNWICK.IO

John Wick Security Lab received the FalconSwap (company/team) FalconSwapCore project smart contract code audit requirements on 2020/12/22.

Project Name: FalconSwapCore

Smart Contract Address:

<https://github.com/FalconSwap/contracts/commit/4c770f410cbe7cb2153f47459986486a0ce9f3f2>

Audit Number: 20201207

Audit Date: 20210107

Audit Category and Result:

Category	Sub-category	Result (Pass/Not Pass)
Contract vulnerability	Integer overflow	Pass
	Race condition	Pass
	Denial of service	Pass
	Logical vulnerability	Pass
	Hardcoded address	Pass
	Function input parameter check	Pass
	Function access control bypass	Pass
	Random number generation	Pass
Random number use	Pass	
Contract specification	Solidity compiler version	Pass
	Event use	Pass
	fallback function use	Pass
	Constructor use	Pass
	Function visibility declaration	Pass
	Variable storage declaration	Pass
	Deprecated keyword use	Pass
	ERC20/223 standard	Pass
ERC721 standard	Pass	
Business risk	Able to arbitrarily create token	Pass
	Able to arbitrarily destroy token	Pass
	Able to arbitrarily suspend tx.	Pass
	"Short address" attack	Pass
	"Fake recharge" attack	Pass
GAS optimization	assert()/require()	Pass
	Loop(for/while) optimization	Pass
	Storage optimization	Pass
Automated fuzzing		Pass

(Other unknown security vulnerabilities and Ethereum design flaws are not included in

this audit responsibility)

Audit Result: **PASS**

Auditor: John Wick Security Lab

(Disclaimer: The John Wick Security Lab issues this report based on the facts that have occurred or existed before the issuance of this report and assumes corresponding responsibility in this regard. For the facts that occur or exist after the issuance of this report, the John Wick Security Lab cannot judge the security status of its smart contracts and does not assume any responsibility for it. The safety audit analysis and other contents of this report are based on the relevant materials and documents provided by the information provider to the John Wick Security Lab when the report is issued (referred to as the information provided). The John Wick Security Lab assumes that there is no missing, falsified, deleted, or concealed information provided. If the information provided is missing, falsified, deleted, concealed, or the information provider's response is inconsistent with the actual situation, the John Wick Security Lab shall not bear any responsibility for the resulting loss and adverse effects.)

Audit Details:

//JohnWick:

```
208: contract FalconSwapCore is Verify, Ownable {  
209:     using SafeMath for uint256;
```

The contract uses the `SafeMath` library to avoid potential integer overflow problems, which is in line with the recommended practice.

After the project's code improvement, no other potential security issues were found in this contract.

Note: The line number of the code involved in the audit details is based on the contract source code uploaded by the project party at etherscan.io or provided by the project party, which is also displayed as a backup in the Smart Contract Source Code section of this report.

Smart Contract Source Code:

According to the confidentiality agreement signed between our party and the project party, this source code is only open to us. If you need to obtain the audited source code, please apply with the project party.

source code link:

```
https://github.com/FalconSwap/contracts/commit/4c770f410cbe7cb2153f47459986486a0ce9f3f2
```