CKB Bitcoin SPV Contracts

Audit Report

Fri May 17 2024

contact@bitslab.xyz

https://twitter.com/scalebit_

ScaleBit

CKB Bitcoin SPV Contracts Audit Report

1 Executive Summary

1.1 Project Information

Description	Bitcoin SPV clients in CKB contracts. A type script for Bitcoin SPV clients.
Type	SPV
Auditors	ScaleBit
Timeline	Tue May 07 2024 - Fri May 17 2024
Languages	Rust
Platform	CKB
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/ckb-cell/ckb-bitcoin-spv-contracts
Commits	b9bfcc6960625d960cf3ce65be974cd75854ae46

1.2 Files in Scope

The following are the SHA1 hashes of the original reviewed files.

ID	File	SHA-1 Hash
UPD	contracts/ckb-bitcoin-spv-type-lock/src/operations/update.rs	7bf13466a5cd38c413397f8928ad4f219de26c74
DES	contracts/ckb-bitcoin-spv-type-lock/src/operations/destroy.rs	04df190c660c89901ed7fa53354fea362b285a0a
CRE	contracts/ckb-bitcoin-spv-type-lock/src/operations/create.rs	58be6aa62601bf7b0f9aac95a85ac55346ae4059
MOD	contracts/ckb-bitcoin-spv-type-lock/src/operations/mod.rs	2a7ad2872946c6a6d880d4982412cc1e854058da
REO	contracts/ckb-bitcoin-spv-type-lock/src/operations/reorg.rs	61c6b6aa462f8fee947654b425f4bcdc747e1347
MAI	contracts/ckb-bitcoin-spv-type-lock/src/main.rs	a16b2103e0c430c0eafe20695509bfad86bf10b1
TID	contracts/ckb-bitcoin-spv-type-lock/src/utilities/type_id.rs	0729cd622edde6b979755455fd2e210837ed4c55
CCBSTLSUMR	contracts/ckb-bitcoin-spv-type-lock/src/utilities/mod.rs	70aa0c3e03f2e83a5d49489548e40c17442c1037
ERR	contracts/ckb-bitcoin-spv-type-lock/src/error.rs	6acee1c2c2f61c83484f5e1ae5f2165e9ff791cf
ENT	contracts/ckb-bitcoin-spv-type-lock/src/entry.rs	bb7b3f0e98f5bf57afb48590eef03725a3e58baa
CCUWOLSMR	contracts/can-update-without-ownership-lock/src/main.rs	f779835f3183423d6b3af95e646e04c601fa93be

CCUWOLSER	contracts/can-update-without-ownership-lock/src/error.rs	03ace876a66c79d3c2e2142f278cf8e85252238a
CCUWOLSER	contracts/can-update-without-ownership-lock/src/entry.rs	11760a98b15a5651957c9364e9852036061ed463

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	2	0	2
Informational	0	0	0
Minor	2	0	2
Medium	0	0	0
Major	0	0	0
Critical	0	0	0

1.4 ScaleBit Audit Breakdown

ScaleBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow
- Number of rounding errors
- Unchecked CALL Return Values
- Functionality Checks
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic issues
- Replay attacks
- Coding style issues

1.5 Methodology

The security team adopted the **"Testing and Automated Analysis"**, **"Code Review"** strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section 1.2.

(3) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by Nervos Network to identify any potential issues and vulnerabilities in the source code of the CKB Bitcoin SPV Contracts smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified 2 issues of varying severity, listed below.

ID	Title	Severity	Status
UPD-1	Missing Timestamp Checking	Minor	Acknowledged
UPD-2	Update an Unchained SPV Cell Causing Subsequent Updates to Stall	Minor	Acknowledged

3 Participant Process

Here are the relevant actors with their respective abilities within the CKB Bitcoin SPV Contracts Smart Contract :

Here are the relevant actors with their respective abilities within the CKB Bitcoin SPV Contracts Smart Contract :

The main role of the contract is to verify that the target transaction has been uploaded to the chain. The verification can be separated into two parts:

(1) Verify whether the given block is already on the chain. (2) Verify that the given transaction is in the given block.

The main purpose of the CKB Bitcoin SPV Contracts contract is to enable the user to verify (1). The contract can provide verification for subsequent RGB++ transactions to help determine whether the corresponding block has been uploaded. In order to achieve the above function, this contract has a service to synchronize the historical blockchain data to the CKB-SPV cell by submitting the updated transaction content. The operation checking is divided into the following four categories (among them, the destroy operation has been temporarily discarded in communication with the developer).

1. Create - Create a set of SPV Instance
2. Destroy -Destroy a set of SPV Instance
3. Update - Update an SPV Instance
4. Reorg - If BTC is reorg, then update a reorg SPV Instanc

4 Findings

UPD-1 Missing Timestamp Checking

Severity: Minor

Status: Acknowledged

Code Location:

contracts/ckb-bitcoin-spv-type-lock/src/operations/update.rs#55

Descriptions:

The SPV Client does not validate the timestamps in the block headers. Attackers can mine privately (without broadcasting to the Bitcoin mainnet), create a block with an arbitrary timestamp, and send it to the SPV Client. There is a brief window of opportunity for an attack before a trusted service uses "reorg" to correct the issue. During this window, the timestamp of the latest block accessed by users is controlled by the attacker, potentially leading to attacks on various transactions that rely on block time. An attacker needs the update privileges of spv-clients to be able to execute an attack. the update privileges of spv-clients are protected by the secp256k1 lock or a corresponding lock. It should also be emphasised that an attacker would need to have mining pool level arithmetic to exploit this vulnerability. This issue has now been confirmed with the project developers and the project developers are considering a fix for a later version.

Suggestion:

1. It is recommended that at least three blocks be updated when performing update and reorg operations.
2. It is advisable to refer to the Bitcoin code for validating timestamps in block headers.

UPD-2 Update an Unchained SPV Cell Causing Subsequent Updates to Stall

Severity: Minor

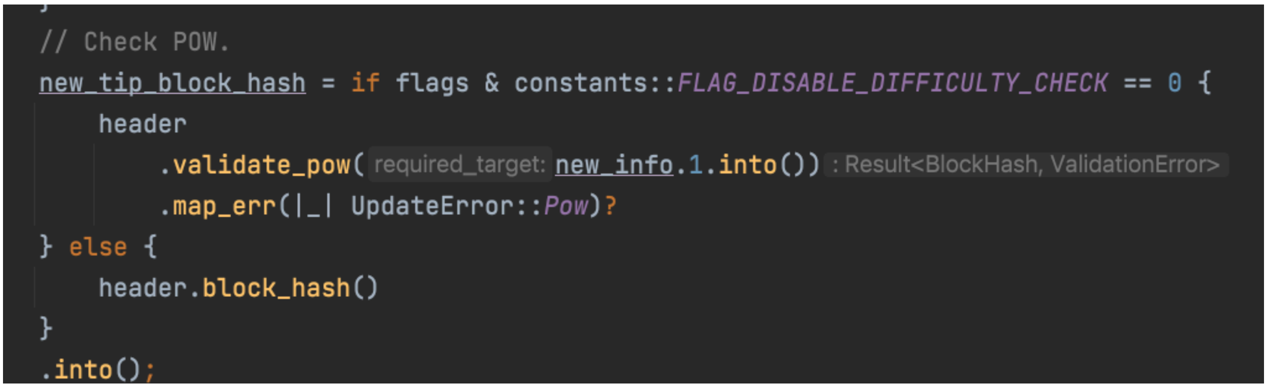
Status: Acknowledged

Code Location:

contracts/ckb-bitcoin-spv-type-lock/src/operations/update.rs#55

Descriptions:

The check faced by this problem is the blockhash difficulty check:



```
// Check POW.
new_tip_block_hash = if flags & constants::FLAG_DISABLE_DIFFICULTY_CHECK == 0 {
    header
        .validate_pow( required_target: new_info.1.into()) : Result<BlockHash, ValidationError>
        .map_err(|_| UpdateError::Pow)?
} else {
    header.block_hash()
}
.into();
```

If the attacker has a certain level of arithmetic that can produce off-link blocks that pass the pow check, it can cause subsequent updates to that contract to stall. An attacker needs the update privileges of spv-clients to be able to execute an attack. The update privileges of spv-clients are protected by the secp256k1 lock or a corresponding lock. It should also be emphasised that an attacker would need to have mining pool level arithmetic to exploit this vulnerability. This issue has now been confirmed with the project developers and the project developers are considering a fix for a later version.

Suggestion:

It is recommended that at least three blocks be updated when performing update and reorg operations.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.