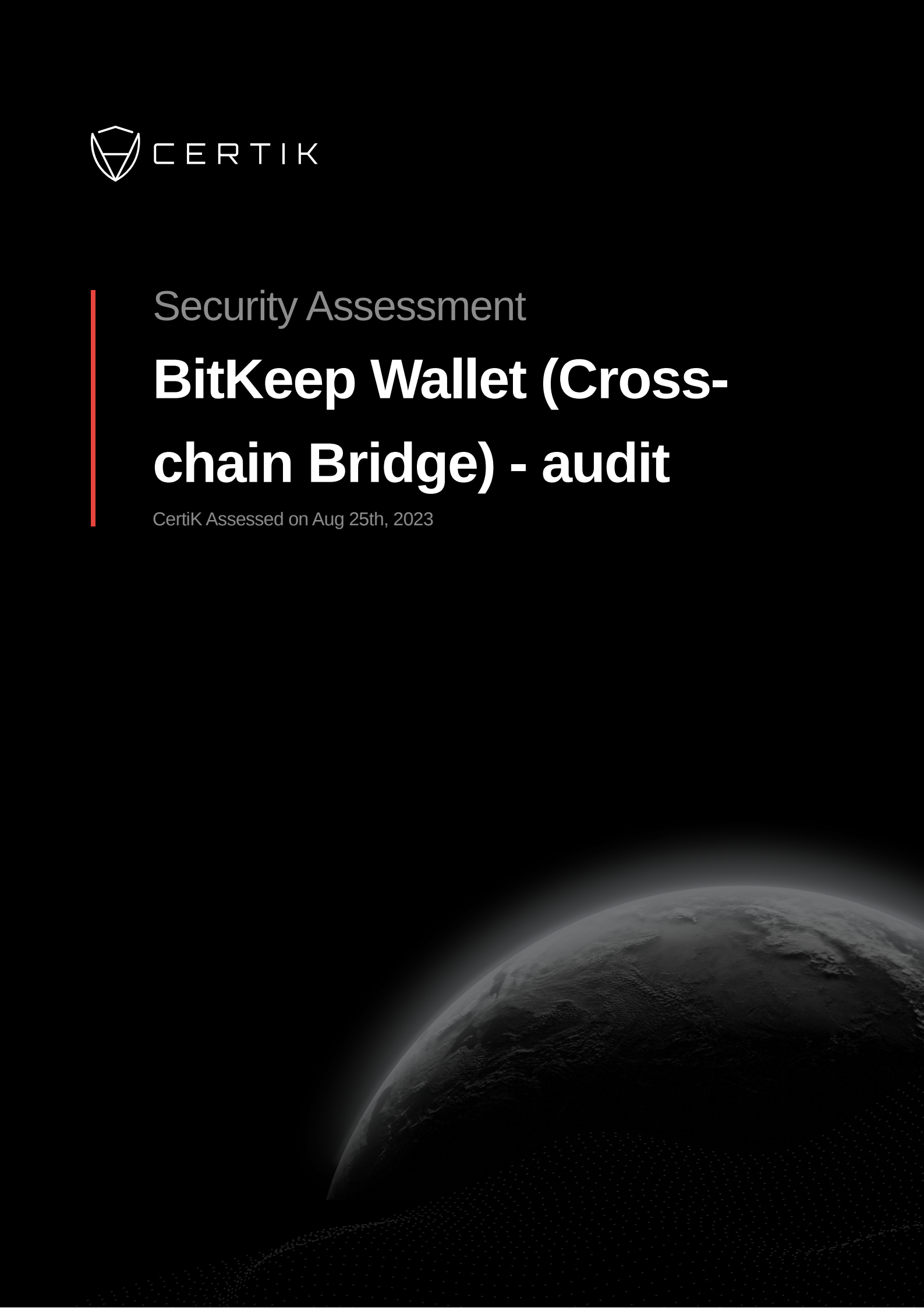
CERTIK

Security Assessment

BitKeep Wallet (Cross-chain Bridge) - audit

CertiK Assessed on Aug 25th, 2023



CertiK Assessed on Aug 25th, 2023

BitKeep Wallet (Cross-chain Bridge) - audit

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Bridge	Ethereum (ETH) | Tron (TRX) | zkSync Era	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 08/25/2023	N/A

CODEBASE
https://github.com/bitkeepwallet/bkbridge
View All in Codebase Page

COMMITS
3cc3020106f2ba35ad0816f1f5273f0ce99f4195
View All in Codebase Page

Vulnerability Summary

9	4	0	0	5	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
2	Major	2 Acknowledged	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
1	Medium	1 Resolved	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
5	Minor	2 Resolved, 3 Acknowledged	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
1	Informational	1 Resolved	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS

BITKEEP WALLET (CROSS-CHAIN BRIDGE) - AUDIT

CODEBASE | BITKEEP WALLET (CROSS-CHAIN BRIDGE) - AUDIT

Repository

https://github.com/bitkeepwallet/bkbridge

Commit

3cc3020106f2ba35ad0816f1f5273f0ce99f4195

AUDIT SCOPE | BITKEEP WALLET (CROSS-CHAIN BRIDGE) - AUDIT

33 files audited ● 6 files with Acknowledged findings ● 3 files with Resolved findings ● 24 files without findings

ID	Repo	File	SHA256 Checksum
BKH	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/libs/BKBridgeHandler.sol	2607eff9f7fbd4bd20948500c857028166dcdb525aece21c7e03478e01706bf5
BKA	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/BKBridgeAccess.sol	314e603530a9c7f8f856879c725b4f231d9ef50a81b76e236190c8307e620c59
BBH	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/libs/BKBridgeHandler.sol	2607eff9f7fbd4bd20948500c857028166dcdb525aece21c7e03478e01706bf5
BKC	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/BKBridgeAccess.sol	6fc7e67089b95b8d6756032389cb2f8c23b236cfbb490d31d343d93bd5f3a2fa
BBP	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/libs/BKBridgeHandler.sol	b797505f2f7d707c1085fbe61a844897073d3f63c1a1e865fa255cc170750787
BKP	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/BKBridgeAccess.sol	314e603530a9c7f8f856879c725b4f231d9ef50a81b76e236190c8307e620c59
BKR	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/BKBridgeRouter.sol	28814c41d5ffb3f6c7e66b612db85f8f029209d406db35ea42133282cac44edf
BKK	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/BKBridgeRouter.sol	3aacbe1ef876c1c4c301b1576ee057f080fd352896bded01312ad451add6a656
BBR	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/BKBridgeRouter.sol	28814c41d5ffb3f6c7e66b612db85f8f029209d406db35ea42133282cac44edf
IBS	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/interfaces/swap/IBKSwap.sol	269a12fff2ce2911a1bca52470b01bb0f97130489b079bb09eeb539a835b05a8
IKS	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/interfaces/swap/IBKSwapRouter.sol	a9e1a328e9db02299b1d04dff4c0c282993aa6987a7fafa58c368c867312574c
IBK	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/interfaces/IBKBridgeAccess.sol	de3982b36bf89a134425970838d6deee7a1e6ce42e7ffbc9f2ede436219cd82d
IBB	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/interfaces/IBKBridgeErrors.sol	78716528f0ad0b11dcbdc334e9a3a7bc1138229ba1b117ac79321d6a53084b25

ID	Repo	File	SHA256 Checksum
IBP	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/interfaces/IBKBridgeParams.sol	c333b46a7bcfeb1299fbdd51f2b5f44420d38ce7824e784b382c8b95f7edefc6
IBR	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/interfaces/IBKBridgeRouter.sol	82cefdded88a57f2726c156fbc09a4037181f5fc8ae06e060660bcbce5160846
BBK	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/libs/BKBridgeKey.sol	a911c78063d3529e0a6fef40adb817793bf03af7c0fc4c562c20cd3be21b1090
THC	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/evm/libs/TransferHelper.sol	fe553357733276ee0e9aeda7aa84e7990b52e2283e4f669a99ff0681fa05520e
IKC	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/interfaces/swap/IBKSwap.sol	269a12fff2ce2911a1bca52470b01bb0f97130489b079bb09eeb539a835b05a8
IKK	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/interfaces/swap/IBKSwapRouter.sol	a9e1a328e9db02299b1d04dff4c0c282993aa6987a7fafa58c368c867312574c
IBA	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/interfaces/IBKBridgeAccess.sol	de3982b36bf89a134425970838d6deee7a1e6ce42e7ffbc9f2ede436219cd82d
IBE	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/interfaces/IBKBridgeErrors.sol	24e52ef45a7af25acebe0ed09f31a6dd8120682549298b56fd51752772be7e62
IBC	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/interfaces/IBKBridgeParams.sol	c68a63ab5d492e95f9f1dad1ac23ab444c2d6c3f566d928636ace7c70dd7cb80
IKB	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/interfaces/IBKBridgeRouter.sol	82cefdded88a57f2726c156fbc09a4037181f5fc8ae06e060660bcbce5160846
BBC	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/libs/BKBridgeKey.sol	a911c78063d3529e0a6fef40adb817793bf03af7c0fc4c562c20cd3be21b1090
THK	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/tron/libs/TransferHelper.sol	fcdb4ae16ab6e743ab8fc80f21c734f2f21795b5d778a67314ee4f26b5fc3118
ISC	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/interfaces/swap/IBKSwap.sol	ec1b8ff3d428b86443d071cf0874e569358245797396d1f938f72a1d60a3cfe1
ISR	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/interfaces/swap/IBKSwapRouter.sol	a9e1a328e9db02299b1d04dff4c0c282993aa6987a7fafa58c368c867312574c
IKA	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/interfaces/IBKBridgeAccess.sol	de3982b36bf89a134425970838d6deee7a1e6ce42e7ffbc9f2ede436219cd82d

ID	Repo	File	SHA256 Checksum
IKE	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/interfaces/IBKBridgeErrors.sol	78716528f0ad0b11dcbdc334e9a3a7bc1138229ba1b117ac79321d6a53084b25
IKP	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/interfaces/IBKBridgeParams.sol	0315d601f6caf43d62057f9deadc9b2d7568373c08d9f18e5f019ded683dce3b
IKR	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/interfaces/IBKBridgeRouter.sol	82cefdded88a57f2726c156fbc09a4037181f5fc8ae06e060660bcbce5160846
BCK	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/libs/BKBridgeKey.sol	a911c78063d3529e0a6fef40adb817793bf03af7c0fc4c562c20cd3be21b1090
THP	CertiKProject/certik-audit-projects	projects/bkbridge/contracts/zksync/libs/TransferHelper.sol	fe553357733276ee0e9aeda7aa84e7990b52e2283e4f669a99ff0681fa05520e

APPROACH & METHODS

BITKEEP WALLET (CROSS-CHAIN BRIDGE) - AUDIT

This report has been prepared for BitKeep Wallet to discover issues and vulnerabilities in the source code of the BitKeep Wallet (Cross-chain Bridge) - audit project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review and Static Analysis techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

FINDINGS | BITKEEP WALLET (CROSS-CHAIN BRIDGE) - AUDIT

9	0	2	1	5	1
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for BitKeep Wallet (Cross-chain Bridge) - audit. Through this audit, we have uncovered 9 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
CON-01	**Potential Transfer Out All Funds**	**Centralization**	**Major**	**Acknowledged**
GLOBAL-01	**Centralization Related Risks**	**Centralization**	**Major**	**Acknowledged**
CON-03	The Signature Can Be Used For Different Orders	Design Issue	Medium	Resolved
BKH-01	Always Refunds The `vaultToken`	Volatile Code	Minor	Acknowledged
CKC-01	Out Of Scope Dependencies	Logical Issue	Minor	Acknowledged
CON-04	Third-Party Dependency Usage	Design Issue	Minor	Acknowledged
GLOBAL-02	Missing Unit-Test File	Volatile Code	Minor	Resolved
THB-01	Unchecked ERC-20 `transfer()` / `transferFrom()` Call	Volatile Code	Minor	Resolved
BBH-01	Incompatibility With Deflationary Tokens	Volatile Code	Informational	Resolved

CON-01 | POTENTIAL TRANSFER OUT ALL FUNDS

Category	Severity	Location	Status
Centralization	**Major**	**projects/bkbridge/contracts/evm/BKBridgeAccess.sol (08/14): 124, 131; projects/bkbridge/contracts/tron/BKBridgeAccess.sol (08/14): 124, 131; projects/bkbridge/contracts/zksync/BKBridgeAccess.sol (08/14): 124, 131**	**Acknowledged**

Description

Based on the logic of this function, the operator has the ability to transfer out all funds in the contract because there is no restriction for the given parameter argument. Although function `rescueERC20` and function `rescueETH` both checks if the `safe` is set to a non-zero address, the owner can change the safe address at any time in function `setAccess` of contract `BKBridgeAccess`.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

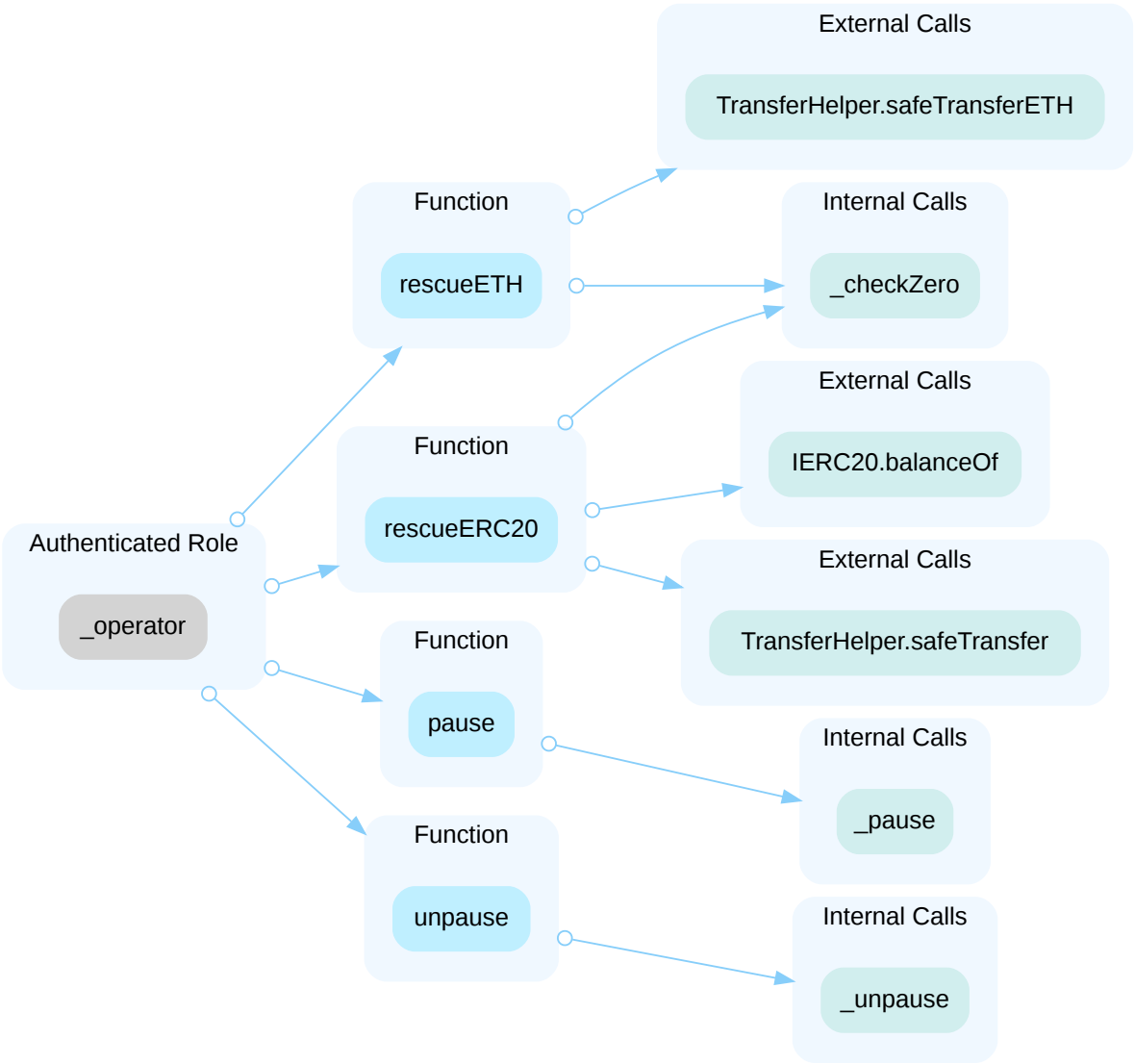
GLOBAL-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	**Major**		**Acknowledged**

Description

In the contract `BKBridgeAccess` the role `_operator` has authority over the functions shown in the diagram below. Any compromise to the `_operator` account may allow the hacker to take advantage of this authority .

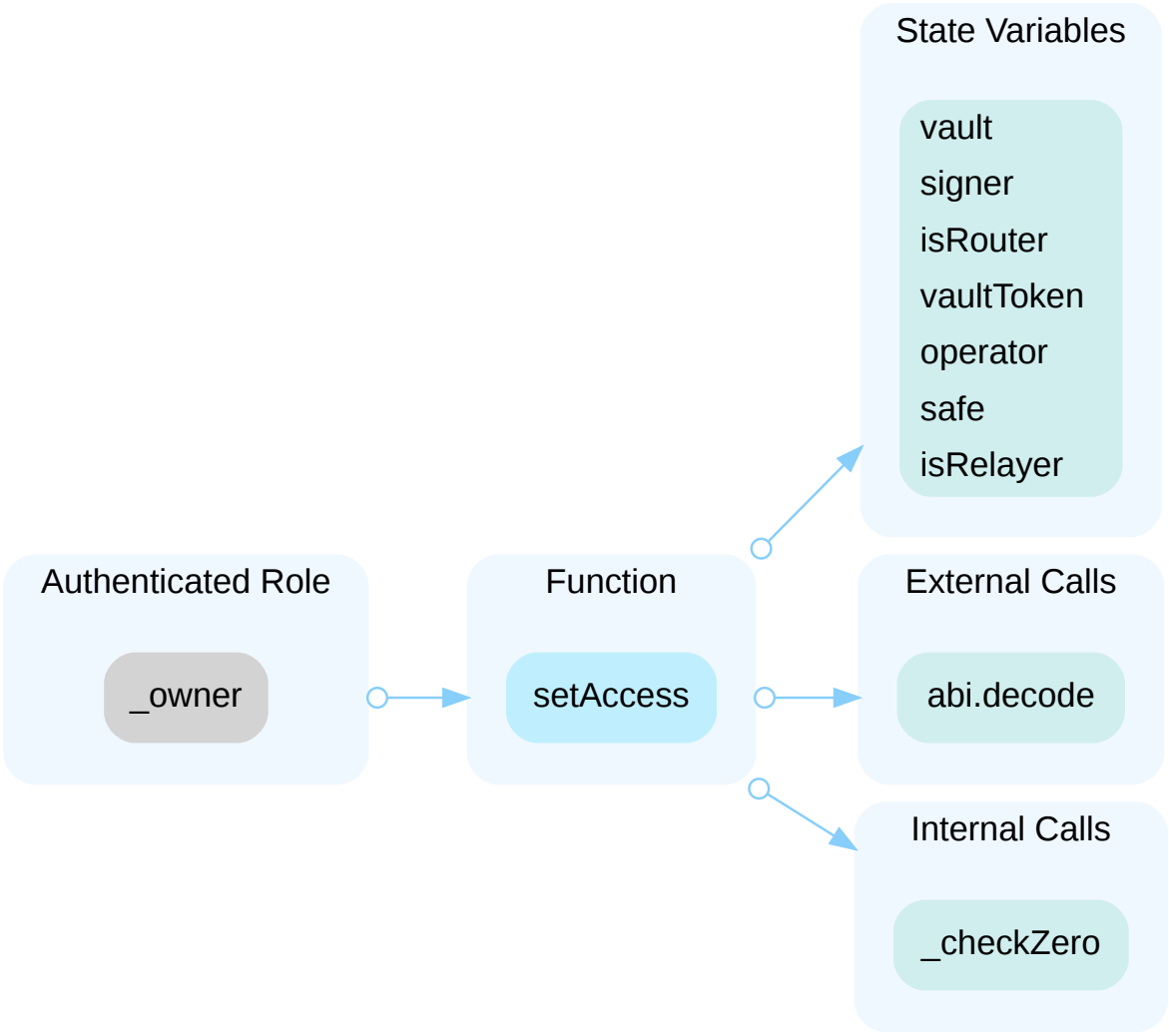
- Withdraw contract's assets through `rescueERC20()` and `rescueETH()`
- Pause or unpause the contract



In the contract `BKBridgeAccess` the role `_owner` has authority over the functions shown in the diagram below. Any

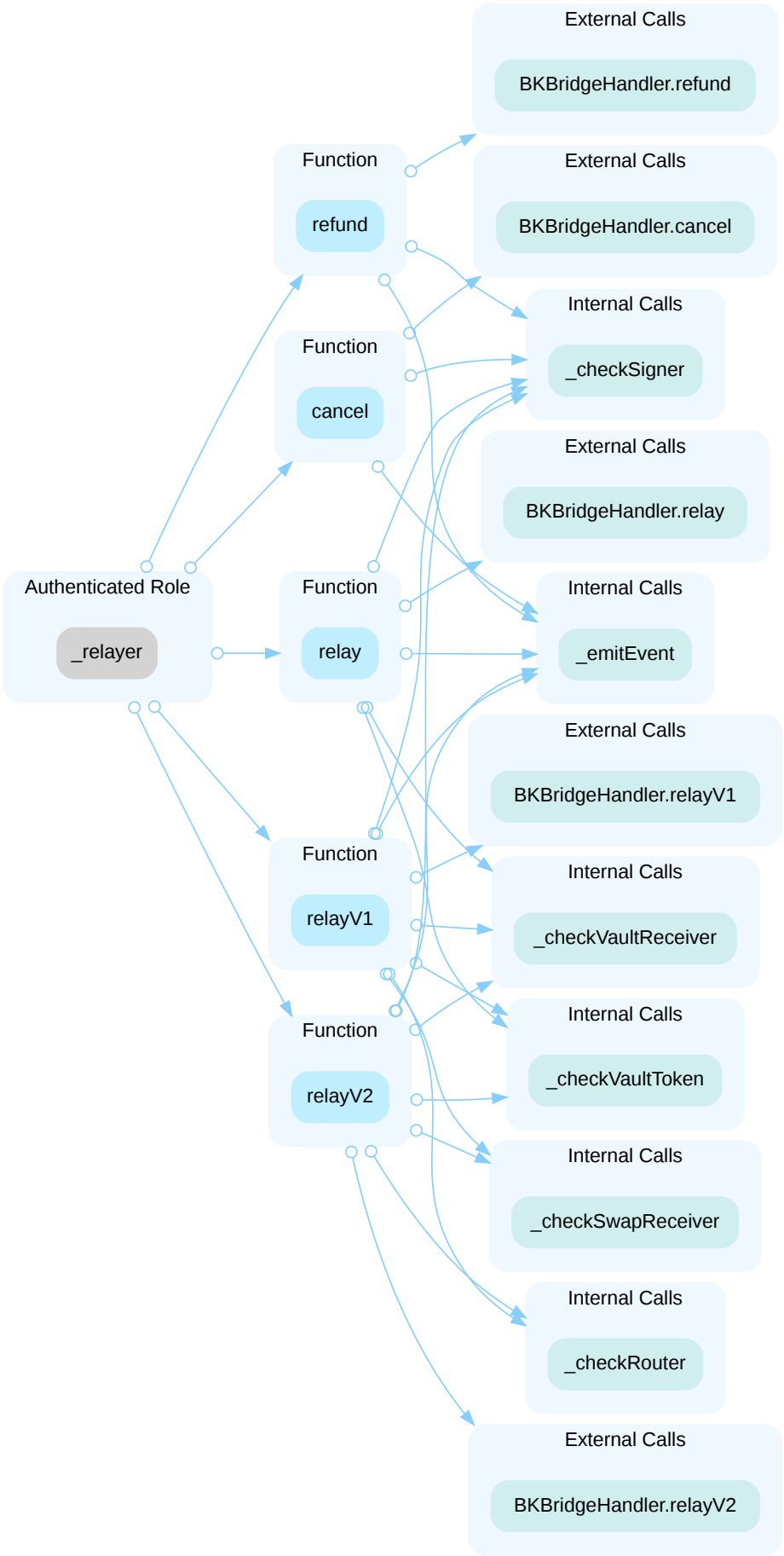
compromise to the `_owner` account may allow the hacker to take advantage of this authority.

- Set the addresses through `setAccess()`



In the contract `BKBridgeRouter` the role `_relayer` has authority over the functions shown in the diagram below. Any compromise to the `_relayer` account may allow the hacker to take advantage of this authority.

- Relay the assets to users through `relay()`, `relayV1()` and `relayV2()`
- Cancel the order through `cancel()`
- Refund the assets to users through `refund()`


External Calls
BKBridgeHandler.refund
Function
refund
External Calls
BKBridgeHandler.cancel
Internal Calls
_checkSigner
Function
cancel
External Calls
BKBridgeHandler.relay
Authenticated Role
_relayer
Function
relay
Internal Calls
_emitEvent
External Calls
BKBridgeHandler.relayV1
Function
relayV1
Internal Calls
_checkVaultReceiver
Function
relayV2
Internal Calls
_checkVaultToken
Internal Calls
_checkSwapReceiver
Internal Calls
_checkRouter
External Calls
BKBridgeHandler.relayV2

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

CON-03 THE SIGNATURE CAN BE USED FOR DIFFERENT ORDERS

Category	Severity	Location	Status
Design Issue	Medium	projects/bkbridge/contracts/evm/BKBridgeRouter.sol (08/14): 40, 54, 70; projects/bkbridge/contracts/tron/BKBridgeRouter.sol (08/14): 41, 56, 73; projects/bkbridge/contracts/zksync/BKBridgeRouter.sol (08/14): 40, 54, 70	Resolved

Description

The signature can be used across different orders. The function `_checkSigner` only checks the `signature` and `nonce`, without taking the `_orderInfo` into considerations. This introduces a potential vulnerability, enabling users to exploit the signature associated with one order for invoking the function with alternative order information. Such an action has the capacity to undermine the intended operational integrity of the project, for example, a user could cancel another user's order by tricking the relayer to call the function `cancel()` passing in another user's order.

Recommendation

We advise the team to include the order infomation into the signed data.

Alleviation

The signature now includes the transfer ID, which is generated off-chain. If an attacker could obtain the transfer ID, it is still possible to using the signature across functions, as he can construct order info with the transfer ID. However, to make the attack profitable, it requires the attacker to trick the relayer to perform certain actions, as the attacker himself can only call send function. The security of the relayer is out of the scope of the audit.

BKH-01 | ALWAYS REFUNDS THE `vaultToken`

Category	Severity	Location	Status
Volatile Code	Minor	projects/bkbridge/contracts/evm/libs/BKBridgeHandler.sol (08/14): 227	Acknowledged

Description

The function `refund()` can be called by anyone to transfer `vaultToken` to `_orderInfo.sender`, but if user deposits other tokens, he can still only get `vaultToken`.

Recommendation

We recommend refunding the assets used by the user across the chain or stating the asset return strategy in the whitepaper.

Alleviation

[Bitkeep Team, 08/25/2023]

This is the project design. The vault only accepts vaultTokens and does not hold any other tokens. Furthermore, it will only refund vaultTokens to users.

CKC-01 | OUT OF SCOPE DEPENDENCIES

Category	Severity	Location	Status
Logical Issue	Minor	$/github/CertiKProject/certik-audit-projects/8ad7142189b3017434290cd93dc0b041a1fd626c/projects/bkbridge/contracts/evm/libs/BKBridgeHandler.sol (08/14): 248, 271; $/github/CertiKProject/certik-audit-projects/8ad7142189b3017434290cd93dc0b041a1fd626c/projects/bkbridge/contracts/tron/libs/BKBridgeHandler.sol (08/14): 248, 271; $/github/CertiKProject/certik-audit-projects/8ad7142189b3017434290cd93dc0b041a1fd626c/projects/bkbridge/contracts/zksync/BKBridgeAccess.sol (08/14): 124; $/github/CertiKProject/certik-audit-projects/8ad7142189b3017434290cd93dc0b041a1fd626c/projects/bkbridge/contracts/zksync/libs/BKBridgeHandler.sol (08/14): 126, 171, 248	Acknowledged

Description

The BKBridgeHandler contracts serve as the underlying entities to interact with contracts `BKSwap` and `BKSwapRouter`. `BKSwap` and `BKSwapRouter` contracts are not in this audit scope. The scope of the audit treats contract that is out of scope as black boxes and assumes their functional correctness. However, in the real world, those contracts can be compromised.

```
248     function _bridgeForSwapV1(SwapV1Info calldata _swapV1Info) internal {
```

- The function `BKBridgeHandler._bridgeForSwapV1` interacts with `BKSwap` contract with `IBKSwap` interface via `_swapV1Info`.

```
271     function _bridgeForSwapV2(SwapV2Info calldata _swapV2Info) internal {
```

- The function `BKBridgeHandler._bridgeForSwapV2` interacts with `BKSwapRouter` contract with `IBKSwapRouter` interface via `_swapV2Info`.

Recommendation

The aforementioned contracts are out of the audit scope. We encourage the team to constantly monitor the status of those contracts and ensure their security and functionality correctness.

Alleviation

[Bitkeep Team, 08/25/2023]

The external projects we rely on have been audited by a professional security audit team, and there are security reports available to prove that they are trustworthy and secure projects.

CON-04 | THIRD-PARTY DEPENDENCY USAGE

Category	Severity	Location	Status
Design Issue	Minor	projects/bkbridge/contracts/evm/BKBridgeAccess.sol (08/14): 124; projects/bkbridge/contracts/evm/libs/BKBridgeHandler.sol (08/14): 126, 171; projects/bkbridge/contracts/tron/BKBridgeAccess.sol (08/14): 124; projects/bkbridge/contracts/tron/libs/BKBridgeHandler.sol (08/14): 126, 171; projects/bkbridge/contracts/zksync/BKBridgeAccess.sol (08/14): 124; projects/bkbridge/contracts/zksync/libs/BKBridgeHandler.sol (08/14): 126, 171, 248, 272	Acknowledged

Description

The contract is serving as the underlying entity to interact with one or more third party protocols. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of third parties can possibly create severe impacts, such as increasing fees of third parties, migrating to new LP pools, etc.

```
124     function rescueERC20(address asset) external onlyOperator {
```

- The function `BKBridgeAccess.rescueERC20` interacts with third party contract with `IERC20` interface via `asset`.

```
171         SwapV2Info calldata _swapV2Info,
```

- The function `BKBridgeHandler.relayV2` interacts with third party contract with `IERC20` interface via `_swapV2Info`.

```
126         SwapV1Info calldata _swapV1Info,
```

- The function `BKBridgeHandler.relayV1` interacts with third party contract with `IERC20` interface via `_swapV1Info`.

Recommendation

The auditors understood that the business logic requires interaction with third parties. It is recommended for the team to constantly monitor the statuses of third parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[Bitkeep Team, 08/25/2023]

The project team has assessed and found no impact on the security of the project.

GLOBAL-02 | MISSING UNIT-TEST FILE

Category	Severity	Location	Status
Volatile Code	Minor		Resolved

Description

Using unit-test to test smart contracts is one of the best ways to identify potential logic errors and security vulnerabilities in the smart contract. No unit-test file was found in the provided GitHub code repository.

Recommendation

We recommend testing the project with comprehensive unit tests before launching on the mainnet.

Alleviation

Testing has been done internally by the client.

THB-01 | UNCHECKED ERC-20 `transfer()` / `transferFrom()` CALL

Category	Severity	Location	Status
Volatile Code	Minor	TransferHelper.sol (3cc3020): 17, 31	Resolved

Description

The return values of the `transfer()` and `transferFrom()` calls in the smart contract are not checked. Some ERC-20 tokens' transfer functions return no values, while others return a bool value, they should be handled with care. If a function returns `false` instead of reverting upon failure, an unchecked failed transfer could be mistakenly considered successful in the contract.

```
17          IERC20(token).transferFrom(from, to, value);
```

```
31          IERC20(token).transfer(to, value);
```

Recommendation

It is advised to use the OpenZeppelin's `SafeERC20.sol` implementation to interact with the `transfer()` and `transferFrom()` functions of external ERC-20 tokens. The OpenZeppelin implementation checks for the existence of a return value and reverts if false is returned, making it compatible with all ERC-20 token implementations.

Alleviation

[BitKeep Team]: USDT token on Tron chain does not return a value when calling function transfer. Using SafeTransfer will cause USDT being unable to transferred on Tron chain.

[CertiK]: The client revised the code and resolved this issue in commit : 471c9acca8d54ae5622355e1dc62ca3a1528a940.

BBH-01 | INCOMPATIBILITY WITH DEFLATIONARY TOKENS

Category	Severity	Location	Status
Volatile Code	Informational	projects/bkbridge/contracts/tron/libs/BKBridgeHandler.sol (08/14): 36, 115, 256, 278	Resolved

Description

When transferring standard ERC20 deflationary tokens, the input amount may not be equal to the received amount due to the charged transaction fee. As a result, an inconsistency in the amount will occur and the transaction may fail due to the validation checks. For example, if a user sends 100 deflationary tokens (with a 10% transaction fee) to the target contract, only 90 tokens actually arrive to the contract.

Recommendation

We advise the client to regulate the set of tokens supported and add necessary mitigation mechanisms to keep track of accurate balances if there is a need to support deflationary tokens.

Alleviation

The client confirms that they do not support deflationary tokens. If user attempts to bridge deflationary tokens, the transfer would revert.

APPENDIX | BITKEEP WALLET (CROSS-CHAIN BRIDGE) - AUDIT

Finding Categories

Categories	Description
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

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

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

CertiK | Securing the Web3 World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.