CERTORA

Aave V3 BTC.b Verification and Listing Stewards Audit

Scope

The scope of the assessment includes two contracts. The first contract is `BridgeToken.sol` (`BTC.b`), which was formally verified. The second contract is `AaveV3AvaBTCBListingSteward.sol`, which was manually audited, as the implementation only calls functions with concrete values. `AaveV3AvaBTCBListingSteward.sol` defines the `BTC.b` configuration on the Aave V3 platform on Avalanche.**

The audit for both contracts was performed by two security engineers and one security researcher, reviewing the code in detail.

The verification of BTCnwas completed on the 28th of June, reviewing the deployed contract on Avalanche.

The audit was completed on the 15th of June, reviewing commit bd1042f of the `BTC.b` listing steward.

Contracts Overview

As part of our continuous formal verification for Aave, we've inspected the `BTC.b` token for security issues and non-trivial features. You can see the results on our Aave dashboard.

The audited contract's purpose is to configure `BTC.b` as a borrowable and collateral token on the Aave V3 platform, on the Avalanche network.

One contract was audited:

1. `AaveV3SAVAXListingSteward.sol`, which configures `sAvax` as a traded token on the AAVE V3 platform. The contract contains two steps:

1.1. Setting a price feed on the AAVE oracle for the `BTCB` token - see in code.

1.2. Listing the token on~~to~~ Aave V3 protocol and configuring it as a borrowable and collateral asset - see in code.

Audit Goals

During the code review, the following checks were performed:

AaveV3SAVAXListingSteward

1. All addresses of the external contracts used match the existing contracts on the Avalanche network.

Correct Setting of Parameters and Values

2. The asset is added to the system correctly, with all the correct `InitReserveInput` struct values. Additional parameters are passed to the correct methods, with the right decimals, e.g. `SUPPLY_CAP`, `RESERVE_FACTOR`, and `LIQ_PROTOCOL_FEE`.

3. The asset is configured as collateral, with proper relations between the LTV, threshold, and liquidation bonus.

Privileges

4. `AaveV3AvaBTCBListingSteward` has the necessary roles to execute `execute()` without reverting.

5. The roles are renounced from the contract at the end of execution.

Findings And Recommendations

Recommendation

Issue:	**Verify that `AaveV3AvaBTCBListingSteward` has the necessary privileges.**
Description:	Many function calls in the listing process require the listing contract to have both `Asset Listing Admin` and `Risk Admin` roles in order to be successfully executed. It is important to remember to grant these roles prior to calling `execute()`.
Recommendation:	Add a dedicated require condition at the beginning of `execute()`, to give a clearer error message if the function reverts for this reason.

Informational

Issue:	The chosen price source is not BTC.b/USD
Description:	The chosen price source for the chainlink oracle is BTC/USD and not BTC.b/USD.
AAVE response :	This is on purpose. The best way of pricing is 1:1 with BTC, followed by PoR.

Informational - Non-Standard Behavior:

1. BTC.b doesn't allow token transfer to its own address.
2. BTC.b has an allowance change on the `burnFrom()` function (by design).
3. The `burnFrom()` function changes the balance of an arbitrary address (by design).
4. A couple of addresses may have privileges to mint BTC.b tokens.

You can see the full results on our AAVE dashboard.

Conclusions

AaveV3SAVAXListingSteward

1. All addresses specified in the contract match existing relevant contracts on the Avalanche blockchain.

Correct Setting of Parameters and Values

2. The asset was added to the system correctly with all the correct `InitReserveInput` struct values, and all parameters are passed to the correct methods, with the right decimals.

3. The asset was configured as collateral with proper relations between the LTV, threshold, and liquidation bonus.

Privileges

4. The roles of the contract are given externally. Therefore, the executor should delegate the necessary privileges before trying to execute.

5. At the end of the process the contract renounces its privileges in the correct manner.

Disclaimer

We hope that this information is useful, but provide no warranty of any kind, explicit or implied. The contents of this report should not be construed as a complete guarantee that the contract is secure in all dimensions. In no event shall Certora or any of its employees be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the results reported here.