Callisto (https://callisto.network)

Monsta Infinite Inception Security Audit

Monsta Infinite Inception security audit, conducted by the Callisto Network Security Department during August 2021.

Monsta Infinite Inception Security Audit Report

Are Your Funds Safe?

Audit Request

The `presale` contract accepts payment in BNB from users to adopt Monsta and allow a `redemption` contract (out of scope of this audit) to redeem Monsta to users.

Contract owner has right to adopt Monsta to any users without payment and limits.

Contract itself does not mint any tokens or other kind of Monsta.

- Website: https://monstainfinite.com/ (https://monstainfinite.com/)
- Twitter: https://twitter.com/monsta_infinite (https://twitter.com/monsta_infinite)
- Telegram: https://t.me/monstainfinite (https://t.me/monstainfinite)

Source code

https://gitlab.com/monsta-infinite/moni-smart-contracts (https://gitlab.com/monsta-infinite/moni-smart-contracts)

Disclosure policy

Standard disclosure policy (https://github.com/EthereumCommonwealth/Auditing/blob/master/Standard_disclosure_policy.md).

Contact

Email : dev@monstainfinite.com (mailto:dev@monstainfinite.com)
Telegram: @jackg0h

Platform

BSC.

1. In scope

Commit 3303268d5456d51a5f7412be8cfca7e3caf73ed5 (https://gitlab.com/monsta-infinite/moni-smart-contracts/-/tree/3303268d5456d51a5f7412be8cfca7e3caf73ed5/contracts)

- /presale/MonstaPresale.sol
- /utils/SafeMath.sol
- /utils/Pausable.sol
- /utils/Ownable.sol

2. Findings

In total, **0 issue** were reported including:

- 0 high severity issue.
- 0 medium severity issue.
- 0 low severity issue.

In total, **5 notes** were reported, including:

- 1 note.
- 4 owner privileges.

No critical security issues were found.

2.1 Owner privileges

Severity: Owner privileges.

Description:

Contract owner has rights:

1. Transfer all BNB held by the contract to the owner using function reclaimBNB (https://gitlab.com/monsta-infinite/moni-smart-contracts/-/blob/3303268d5456d51a5f7412be8cfca7e3caf73ed5/contracts/presale/MonstaPresale.sol#L93).
2. Giveaway (https://gitlab.com/monsta-infinite/moni-smart-contracts/-/blob/3303268d5456d51a5f7412be8cfca7e3caf73ed5/contracts/presale/MonstaPresale.sol#L79) Monsta without effecting adopted Monsta counter to any addresses without payment.
3. Pause/unpause `MonstaPresale` contract.
4. Set (https://gitlab.com/monsta-infinite/moni-smart-contracts/-/blob/3303268d5456d51a5f7412be8cfca7e3caf73ed5/contracts/presale/MonstaPresale.sol#L60) redemption contract address.

2.2 Contract logic is not completed

Severity: Note.

Description:

There is a function redeemAdoptedMonsta (https://gitlab.com/monsta-infinite/moni-smart-contracts/-/blob/3303268d5456d51a5f7412be8cfca7e3caf73ed5/contracts/presale/MonstaPresale.sol#L68-74) that can be called from redemption contract only, but there is not code of this contract in the provided repository. So entire logic of this function is not clear.

3. Security practice

- ☑ **Open-source contact**.
- ☐ **The contract should pass a bug bounty after the completion of the security audit.**
- ☐ **Public testing.**
- ☐ **Automated anomaly detection systems.** – NOT IMPLEMENTED. A simple anomaly detection algorithm is recommended to be implemented to detect behavior that is atypical compared to normal for this contract. For instance, the contract must halt deposits in case a large amount is being withdrawn in a short period of time until the owner or the community of the contract approves further operations.
- ☐ **Multisig owner account.**
- ☐ **Standard ERC20-related issues.** – NOT IMPLEMENTED. It is known that every contract can potentially receive an unintended ERC20-token deposit without the ability to reject it even if the contract is not

intended to receive or hold tokens. As a result, it is recommended to implement a function that will allow extracting any arbitrary number of tokens from the contract.

- ☐ **Crosschain address collisions.** ETH, ETC, CLO, etc. It is possible that a transaction can be sent to the address of your contract at another chain (as a result of a user mistake or some software fault). It is recommended that you deploy a "mock contract" that would allow you to withdraw any tokens from that address or prevent any funds deposits. Note that you can reject transactions of native token deposited, but you can not reject the deposits of ERC20 tokens. You can use this source code as a mock contract: extractor contract source code (https://github.com/EthereumCommonwealth/GNT-emergency-extractor-contract/blob/master/extractor.sol). The address of a new contract deployed using `CREATE (0xf0)` opcode is assigned following this scheme `keccak256(rlp([sender, nonce]))`. Therefore you need to use the same address that was originally used at the main chain to deploy the mock contract at a transaction with the `nonce` that matches that on the original chain. *Example: If you have deployed your main contract with address 0x010101 at your 2021th transaction then you need to increase your nonce of 0x010101 address to 2020 at the chain where your mock contract will be deployed. Then you can deploy your mock contract with your 2021th transaction, and it will receive the same address as your mainnet contract.*

4. Conclusion

The audited smart contract can be deployed. No security issues were found in the audited contracts. Pay attention, the `redemption` contract was not included in the audit and its logic is unknown.

It is recommended to adhere to the security practices described in pt. 4 of this report to ensure the contract's operability and prevent any issues that are not directly related to the code of this smart contract.

Appendix

Smart Contract Audits by Callisto Network. (https://callisto.network/smart-contract-audit/)

Miscellaneous

Why Audit Smart Contracts? (https://callisto.network/why-audit-smart-contracts/)

Our Most Popular Audit Reports. (https://callisto.network/security-audits/)

Blockchain as Seen by Security Experts.

Follow Callisto's Security Department on Twitter (https://twitter.com/Callisto_Audits) to get our latest news and updates!

Published on **August 27, 2021**

(https://callisto.network/monsta-infinite-infinite-infinite-infinite-infinite-infinite-inception-inception-inception-inception-inception-inception-security-security-security-security-security-security-audit/) audit/) audit/) audit/) audit/) audit/)

Security Audits (https://callisto.network/tag/security-audits/)

‹ Previous post (https://callisto.network/defifarms-protocol-security-audit/) Next post ›

Callisto Network LTD

71-75 Shelton Street
London, Greater London
United Kingdom, WC2H 9JQ

Join Our Community

(https://t.me/CallistoNet) (https://twitter.com/CallistoSupport) (https://reddit.com/r/CallistoCrypto) (https://www.youtube.com/channel/UC1WMae32v_eJ8qOtLQqM26Q)

(https://www.instagram.com/callisto.network/) (https://www.facebook.com/callistonetwork) (https://www.linkedin.com/company/callisto-network/) (https://t.co/DAWunSR1tm)

Resources

FAQ (https://callisto.network/faq/)

Timeline (https://callisto.network/timeline/)

Airdrop (https://callisto.network/callisto-airdrop/)

Community Guidelines (https://callisto.network/community-guidelines/)

Callisto

Partners (https://callisto.network/partners/)

Our GitHub repositories (https://github.com/EthereumCommonwealth)

Media Kit (https://github.com/EthereumCommonwealth/Callisto-Media-Kit)

Contact us (https://callisto.network/contact-us/)

Want to sell your CLO coins OTC? (mailto:vladimir.vencalek@invictussolutions.cz)