callisto

Bitcademy Audit Report

Contents

1. Summary

Bitcademy V4 security audit report performed by Callisto Security Audit Department

2. In scope

- BitcademyToken.sol github commit hash 3d5e341ca04b20e4ea4f93a9a28e106a38571e36.
- BitcademyVesting.sol github commit hash 072d747e38ba5da87a021bcf2758be62b9795477.
- Crowdsale.sol github commit hash ff59c42210cf5f8c336de7e36ffc76e31c38e7d7.
- PreICOBitcademyGold.sol github commit hash ff59c42210cf5f8c336de7e36ffc76e31c38e7d7.
- RefundVault.sol github commit hash ff59c42210cf5f8c336de7e36ffc76e31c38e7d7.

3. Findings

In total, **2 issues** were reported including:

- 2 low severity issues.

3.1. ICO Autonomy

Severity: low

Description

- `updateReleaseDate` function allow the contract owner to extend the token locking period, making the investors wait more to be able to withdraw their tokens.
- `adjustCloseDate` function allow the contract owner to extend the ICO close time. For example if the owner private key is hacked, an attacker can set the `closingTime` value so far into the future that `finalize` function will throw at each call. all the fund collected fund and tokens will be locked.

Many consequences can be described concerning the above issue, contract developers should make the ICO as autonomous as possible.

This issue is applicable for both `Crowdsale` and `PreICOBitcademyGold` contracts.

Code snippet

https://github.com/yuriy77k/Bitcademy_ICO/blob/ff59c42210cf5f8c336de7e36ffc76e31c38e7d7/contracts/Crowdsale.sol#L546

https://github.com/yuriy77k/Bitcademy_ICO/blob/ff59c42210cf5f8c336de7e36ffc76e31c38e7d7/contracts/Crowdsale.sol#L555

https://github.com/yuriy77k/Bitcademy_ICO/blob/ff59c42210cf5f8c336de7e36ffc76e31c38e7d7/contracts/PreICOBitcademyGold.sol#L429

https://github.com/yuriy77k/Bitcademy_ICO/blob/ff59c42210cf5f8c336de7e36ffc76e31c38e7d7/contracts/PreICOBitcademyGold.sol#L438

3.2. Known vulnerabilities of ERC-20 token

Severity: low

Description

1. It is possible to double withdrawal attack. More details here
2. Lack of transaction handling mechanism issue. WARNING! This is a very common issue and it already caused millions of dollars losses for lots of token users! More details here

4. Conclusion

The audited contracts are safe to deploy.