Audius Contracts Audit

AUGUST 25, 2020 | IN SECURITY AUDITS | BY OPENZEPPELIN SECURITY

Conclusions

3 critical and 12 high severity issues were found. Some changes were proposed to follow best practices and reduce potential attack surface.

Update: *The Audius team fixed all the critical, high, and medium severity issues that we reported.*

Additional security recommendations

Note*: The following recommendations were made after the Audius team had already addressed the issues from our initial audit.*

Audius has a lot of moving parts: A delegated staking system, a rewards program, a registration system, a voting and governance system, and a slashing mechanism. The code to implement all these moving parts is complex, and there are a lot of interactions between the various systems. We have done our best to raise as many valuable security issues as we could find during our time-limited engagement. However, we cannot guarantee that we've found all the bugs or enumerated all the risks in the Audius system.

Given the complexity of this system, and the large number of users that may interact with it, consider applying the following recommendations to further reduce the attack surface, mitigate risk, and get more eyes on the code:

- Beta testing: Consider engaging a community of early adopters to put the system under test with conditions as close to mainnet as possible.
- Bug bounty: Consider implementing a bug bounty program to get more eyes on the code, and to incentivize hackers to contribute with the system instead of attacking it.
- Future reaudit: Given the high number of critical and high severity issues found during this audit, the number of changes that were made as a result, and the complex interactions between the various systems, we suggest the Audius team to analyze the results of the beta testing and bug bounty to decide if the code should be reaudited with a fresh set of eyes.
- Security contact info: To make it easier for independent security researchers to contact Audius with any issues they may find, consider adding security contact info to the `audius-protocol` repo and/or the Audius website.

< PREVIOUS

Security Audits

- If you are interested in smart contract security, you can continue the discussion in our forum, or even better, join the team 🚀
- If you are building a project of your own and would like to request a security audit, please do so here.

RELATED POSTS

SECURITY AUDITS

Balancer Contracts Audit

Balancer is an automated portfolio manager. It allows anyone to create Balancer pools, each of...

READ MORE

by OpenZeppelin Security

SECURITY AUDITS

Opyn Contracts Audit

The Opyn team asked us to review and audit the system. We looked at the code and now publish our...

READ MORE

by OpenZeppelin Security

SECURITY AUDITS

Aave Protocol Audit Summary

The Aave team asked us to review and audit a pre-production version of their protocol.

READ MORE

by OpenZeppelin Security