Reporte ejecutivo de la auditoría del Smart Contract principal (rev. 2)

Bamboo

10-26-2020

1. Introducción

Esta es una de las auditorías parciales, en este caso, realizada sobre el Smart Contract principal de **BAMBOO DEFI** donde se encontraron varias mejoras que se podían implementar.

El ecosistema **BAMBOO DEFI** está formado por una gran cantidad de Smart Contracts que interactúan entre sí. Todos ellos van a ser auditados por **Red4Sec** y una vez que depurados los posibles errores y se apliquen las mejoras recomendadas, será otorgado el sello aprobatorio de calidad.

2. Trabajo realizado hasta esta segunda revisión

Tras la entrega del primer informe de la auditoría de **Red4Sec**, el equipo de desarrollo de **BAMBOO DEFI** ha aplicado los siguientes procedimientos.

1. Solución del problema de burn tokens delegados
2. Implementamos la mejora en el proceso de cambiar el ownership del SC principal para dejarlo en manos del SmartContract
3. Incorporación de la licencia MIT a todos los contratos
4. Refactorización del código para mejorar su legibilidad
5. Corrección del blocktype mencionado en la auditoría (rev.1)
6. Refactorización de funciones para optimizar el consumo de gas
7.

3. Tabla de resultados

En los siguientes datos se refleja la segunda auditoría, publicada el 26 de octubre de 2020, a la que ha estado expuesto el código de Smart Contract principal de **BAMBOO DEFI**.

Vulnerability	State	Notes
Unlimited designation votes	Fixed	
Unbounded Loop in getPriorVotes method	Assumed	
Unsecure Ownership Transfer	Fixed	
Block number stored in a wrong type	Fixed	
GAS Optimization	Assumed	
Improvable Code Quality	Partially fixed	
Absence of Unit Test	Assumed	
Outdated Third-Party Libraries	Fixed	
Provide License for Third-Party Code	Assumed	

4. Anotaciones del equipo de desarrollo

Nexxyo Labs ha considerado por el bien del proyecto que es positivo mantener la idea sobre el desarrollo inicial acerca de dos puntos mencionados en la auditoría de **Red4Sec**.

Unbounded Loop in getPriorVotes method

Es la mejor manera de implementar esta función. Se ha llevado a cabo un análisis técnico en diferentes protocolos de tecnología Blockchain y todos ellos concluyen en utilizar la misma función. Considerándose su utilización como un estándar.

Innecesaria actualización de los contratos de OpenZepellin

Esta decisión es tomada como relevante puesto que prefiere utilizar la versión de Solidity 0.6.12. Versión, a su vez, implementada en proyectos de gran calado como **Uniswap** y **SushiSwap**.

5. Progresión tras esta inicial auditoría

Continuando con el desarrollo del proyecto, el equipo de **BAMBOO DEFI**, ha publicado los contractos del DEX, STAKING y periféricos en la red Testnet de Ethereum. Encontrándose pendientes de que **Red4Sec** los audite. Avanzando, a su vez, con diferentes otras partes y aspectos relevantes del proyecto:

- ✓ Unit test staking
    - Superar la auditoria de este contrato
- ✓ Raindrop
    - Unit test raindrop
    - Superar la auditoria de este Smart Contrat
- ✓ Conectar el frontend de la plataforma web a la red Testnet
    - Test intensivos en la red Testnet
- ✓ Publicación de todos los contratos en la red Mainnet
- ✓ Publicación del frontend web en la red Mainnet

Una vez cumplidas las fases de trabajo anteriores, **Red4Sec** va a llevar a cabo una revisión global del proyecto y tras su autorización será entregado el certificado a **BAMBOO DEFI**.

¡Haz crecer tu panda interior!

BambooDeFi.com