Informe de Auditoría: Smart Contract “NFT Marketplace”

Fecha: 5 de Julio de 2023

Fuente:

https://github.com/HalbornSecurity/CTFs/tree/master/HalbornCTF_Solidity_Ethereum/CTF1_NFTMarketplace

Resumen Ejecutivo:

Hemos auditado un contrato inteligente de Ethereum que implementa la compraventa y subasta de tokens no fungibles (NFTs) y hemos identificado tres fallas de seguridad importantes. A continuación, detallamos los problemas y recomendamos soluciones.

Robo de tokens APE en la ejecución de una orden de compra:

El primer problema identificado permite al propietario de un NFT robar tokens APE del contrato, después de que un usuario haya puesto una orden de compra por el NFT. Esto se logra creando otra orden de compra desde una dirección auxiliar, realizando la venta a la dirección auxiliar, devolviendo el NFT al propietario, y realizando de nuevo la venta a la dirección auxiliar, utilizando los tokens APE adicionales que fueron depositados por el primer ordenante. La función sellToOrderId() no verifica correctamente si la orden ya ha sido ejecutada, lo que permite este ataque.

Recomendación: Se debe corregir la verificación de estado en la función sellToOrderId(). La función debe comprobar correctamente si la orden ya ha sido ejecutada para prevenir la venta múltiple del mismo NFT.

Robo de tokens APE por cancelación indebida de la orden de compra:

El segundo problema es similar al primero, un usuario crea una orden de compra y el atacante crea otra orden igual desde una dirección auxiliar, pero en este caso, después de realizarse la venta del NFT a la dirección auxiliar, esta cancela la orden de compra de forma indebida y recupera los tokens APE depositados, utilizando los tokens APE que fueron depositados por el primer ordenante. La función cancelBuyOrder() no verifica correctamente si la orden de compra ya ha sido ejecutada, lo que permite este ataque.

Recomendación: Se debe corregir la verificación de estado en la función cancelBuyOrder(). La función debe comprobar correctamente si la orden ya ha sido ejecutada para prevenir la cancelación de órdenes ya ejecutadas.

Ataque de denegación de servicio (DoS) en la función bid():

El tercer problema identificado es un ataque de denegación de servicio (DoS) a través de la función bid(). Un usuario puede colocar una oferta por un NFT o por todos los NFTs de la colección, por un precio mínimo, mediante un Smart contract malicioso. El problema radica en el uso de la función call() que devuelve los fondos al oferente anterior. El Smart contract malicioso puede bloquear esta devolución, impidiendo que se realicen nuevas pujas.

Recomendación: El problema se puede mitigar ignorando el error en caso de no poder devolverse los fondos al oferente anterior. Esto garantizará que las operaciones de subasta continúen sin interrupciones.

Esperamos que las recomendaciones presentadas en este informe sean de utilidad para mejorar la seguridad y la fiabilidad del contrato inteligente analizado. Estamos a disposición para cualquier consulta o asistencia adicional que se requiera.