Informe de Auditoría de Smart Contract “Halborn Token”

Fecha: 6 de Julio, 2023

Fuente:

https://github.com/HalbornSecurity/CTFs/tree/master/HalbornCTF_Solidity_Ethereum/CTF2_HalbornToken

Resumen Ejecutivo:

En nuestra reciente auditoría del smart contract de Ethereum, hemos identificado tres problemas principales que potencialmente ponen en peligro la integridad y seguridad del contrato. Los errores implican funciones de minting de tokens, asignación de signers y control de vesting, que pueden ser explotadas para beneficio no autorizado.

Error en la función setSigner()

Hemos identificado un error crítico en la función setSigner(). Esta función permite que cualquier usuario se posicione como signer. Una vez que un usuario se convierte en signer, tiene la capacidad de crear tokens de manera ilimitada utilizando la función mintTokensWithSignature(), generando una firma ECDSA con su clave privada. Este problema da potencial para la creación indebida de tokens y una devaluación masiva del mismo.

Recomendación: Asegurarse de que sólo el actual signer puede llamar a la función setSigner().

Error en los parámetros de la función mintTokensWithWhitelist()

Hemos descubierto un error en los parámetros de la función mintTokensWithWhitelist(). Esta función actualmente acepta el valor de Merkle root como un parámetro, a pesar de que este valor se configura durante la construcción del contrato y no debería poder ser modificado después. Permitir que este valor sea enviado con la llamada a la función permite a cualquier usuario generar una prueba Merkle para su propia dirección de billetera y mintear crear nuevos tokens de forma indebida.

Recomendación: La función mintTokensWithWhitelist() debe ser modificada para eliminar el parámetro Merkle root y usar el que se establece en el constructor.

Control del Vesting en manos de los usuarios

El control del vesting ha sido puesto en manos de los usuarios. Esto es problemático ya que permite a los usuarios alterar las condiciones de su período de vesting, algo que solo el propietario del contrato debería poder hacer.

Recomendación: La capacidad de activar el vesting debe ser restringida al propietario del contrato.

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.