halborn.com

Explained: The BurgerSwap Hack (May 2021)

2-3 minutos

On May 28, 2021, the Binance Smart Chain (BSC)-based BurgerSwap protocol experienced a flash loan attack. The attacker of the DeFi protocol managed to steal approximately $7.2 million in tokens by manipulating the price of the BURGER token.

How the Attack Worked

The hack on BurgerSwap was based on a fake token contract and a reentrancy exploit. The attack began and ended with a flash loan from PancakeSwap that provided the source of the funds used in the attack.

With the tokens gained from the flash loan, the attacker took the following steps (using WBNB as an example):

1. Created a fake token and a trading pair between BURGER and the fake token
2. Created a routing of BURGER -> fake token -> WBNB using the new trading pair between BURGER and the fake token

3. Traded WBNB from the flash loan to BURGER on BurgerSwap
4. Manipulated the price of $BURGER by adding 100 fake tokens and 4.5k BURGER to the pool
5. Converted 100 fake tokens to 4,400 WBNB using the pool
6. Used reentrancy to swap another 45k BURGER for 4.4k $WBNB
7. Swapped 493 WBNB for $108,700 in $BURGER tokens

By using this technique, the attacker was able to steal a number of different altcoins as well as over $4 million in BURGER and xBURGER. The total theft is valued at about $7.2 million.

Lessons Learned from the Attack

The BurgerSwap hack is the latest in a series of attacks on DeFi protocols that take advantage of price manipulation. Since many DeFi liquidity pools base their exchange rates on the relative amounts of the tokens in a trading pair that they contain, manipulation of these amounts changes the rates and allows attackers to extract more value than they put in. **Flash loans make these attacks easy to perform by providing the seed capital needed to manipulate prices and achieve large gains.**

This and previous attacks on DeFi protocols have demonstrated the risks of calculating exchange rates within the code of a smart contract. Preventing future attacks requires the use of an external reference for

exchange rates that is less vulnerable to manipulation.