SharkTeam

Flash Loan and Re-entry Attack: Analysis of Grim Finance's Hacked Event

Dec 20th, 2021

On January 19, time on January 19, Fantom Finance suffered a lightning attack and lost more than 30 million US dollars. Grim Finance has all the vaults and reminded users to stop withdrawing their personal assets in time.

SharkTeam conducted an analysis and technical analysis of this incident, and concluded a security measure. It is hoped that chain projects in the chain industry can learn from this and build a blockchain security defense line.

1.Event analysis

During the entire attack process, the attackers attacked multiple LP vault contracts and single-currency vault contracts of Grim Finance, including the following transactions:

Finally, the obtained token will be transferred to other public chains through AnySwap cross-chain transfer. For example, the FTM cross-chain transaction is as follows:

Taking transaction 0x19315e5b150d0a83e797203bb9c957ec1fa8a6f404f4f761d970cb29a74a5dd6 as an example, the detailed description of the attack project is as follows:

1. Flash loans and add liquidity. Borrow 937830 WFTM and 30 BTC through a flash loan, then add liquidity to the WFTM/BTC Pancake trading pair to get 0.0476 SPIRIT-LP liquidity certificate.

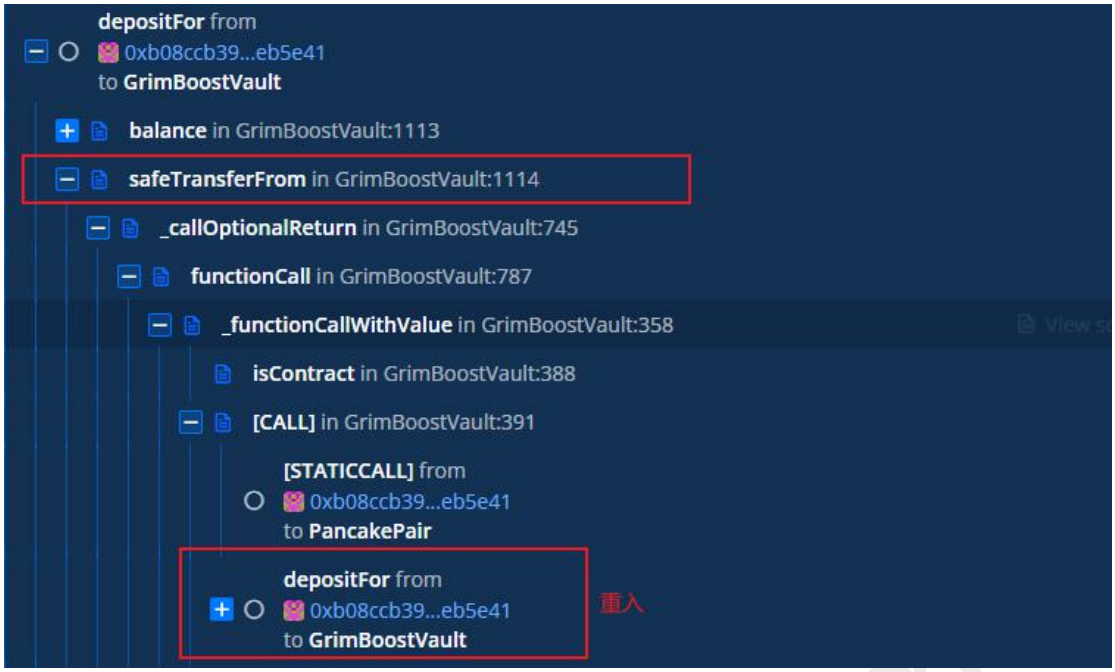
2. Pledge liquidity vouchers to the vault contract and mint share tokens.

The attack contract pledged the liquidity token to the vault through the depositFor function in the GrimBoostVault contract, and minted 316 GB-BTC-FTM share tokens.

```
1115    function depositFor(address token, uint _amount,address user ) public {
1116
1117        uint256 _pool = balance();
1118        IERC20(token).safeTransferFrom(msg.sender, address(this), _amount);
1119        earn();
1120        uint256 _after = balance();
1121        _amount = _after.sub(_pool); // Additional check for deflationary tokens
1122        uint256 shares = 0;
1123        if (totalSupply() == 0) {
1124            shares = _amount;
1125        } else {
1126            shares = (_amount.mul(totalSupply())).div(_pool);
1127        }
1128        _mint(user, shares);
1129    }
```

In this process, because the depositFor function does not verify the parameter token, that is, any token can be passed to mint share tokens, and the attacker contract can mint share tokens by passing a custom token contract (attack contract address).

The reentrancy of the depositFor function is implemented multiple times through the safeTransferFrom function in the custom token contract.



Pass the correct WFTM/BTC SPIRIT-LP transaction pair address and 0.0476 SPIRIT-LP in the last reentrant call to the depositFor function.

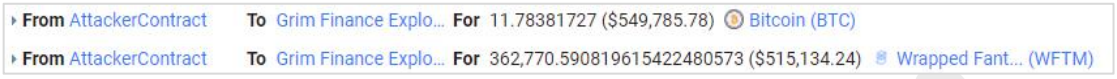
This repeated minting of share tokens eventually allowed the GrimBoostVault contract to mint far more share tokens (316 GB-BTC-FTM) for the attacker than expected.

3. Withdraw liquidity certificates based on share tokens.

The attack contract has withdrawn 0.0663 SPIRIT-LP based on the minted far more tokens than expected (316 GB-BTC-FTM), which is significantly more than the actual pledged 0.0476 SPIRIT-LP.

4. Remove liquidity and repay the flash loan.

5. Transfer the remaining 362,770 WFTM and 11.78 BTC to the attacker's account address.



The root cause of this attack is: because the depositFor function in the Grim contract does not verify the parameter token, that is, any token can be passed to mint share tokens. The attacker mints share tokens by passing a custom token contract (attack contract address), and re-enters the depositFor function through the safeTransferFrom function in the custom token contract, which eventually causes the GrimBoostVault contract to mint far more than expected for the attacker of share tokens (316 GB-BTC-FTM).

2. safety recommendations

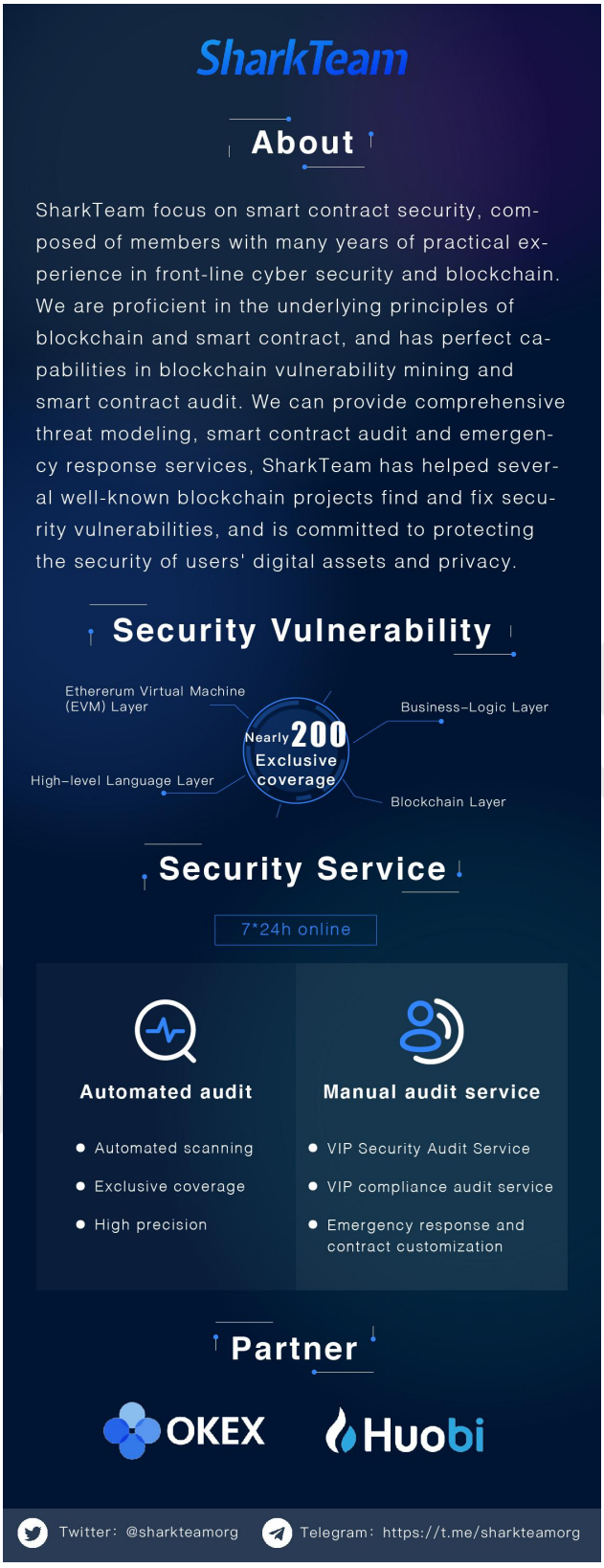
This incident is another security incident related to lightning loans. The business logic design of the DeFi project is complex, involving many economic calculations and parameters, but the composability between different projects and agreements is extremely rich and difficult to predict. Prone to security breaches. As shown in the table below, the number of DeFi incidents that used

flash loans to attack this new product has been endless in the past year, which has increased to 46. Generally, lightning loan attacks include four types: "raising arbitrage," "oracles manipulation," "re-entry attacks," and "technical vulnerabilities." This is a lightning loan attack based on the use of "oracles".

编号	日期	主攻协议	闪电贷协议	攻击类型
1	2020/2/15	bZx	dYdX	哄抬套利
2	2020/2/18	bZx	bZx	操纵预言机
3	2020/6/28	Balancer	dYdX	哄抬套利
4	2020/10/26	Harvest	Uniswap V2	操纵预言机
5	2020/11/6	Cheese Bank	dYdX	操纵预言机
6	2020/11/12	Akropolis	dYdX	重入攻击
7	2020/11/14	Value.DeFi	Aave/Uniswap V2	操纵预言机
8	2020/11/17	OUSD	dYdX	重入攻击
9	2020/12/18	Warp Finance	Uniswap V2/dYdX	操纵预言机
10	2021/2/4	Yearn.Finance	dYdX/Aave	哄抬套利
11	2021/2/13	Alpha.Finance	Aave	技术漏洞
12	2021/5/2	Spartan	PancakeSwap	哄抬套利
13	2021/5/8	Value.DeFi	Value.DeFi	技术漏洞
14	2021/5/8	Rari Capital	dYdX	重入攻击
15	2021/5/13	xToken	dYdX	操纵预言机
16	2021/5/16	bEarn Fi	Cream.Finance	技术漏洞
17	2021/5/20	PancakeBunny	PancakeSwap	操纵预言机
18	2021/5/22	Bogged Finance	PancakeSwap	技术漏洞
19	2021/5/25	AutoShark	PancakeSwap	技术漏洞+操纵预言机
20	2021/5/28	BurgerSwap	PancakeSwap	重入攻击
21	2021/5/28	JulSwap	JulSwap	操纵预言机
22	2021/5/30	Belt Finance	PancakeSwap	操纵预言机
23	2021/6/5	BurgerSwap	PancakeSwap	重入攻击
24	2021/6/10	EvoDeFi	PancakeSwap	技术漏洞
25	2021/6/19	Impossible Finance	PancakeSwap	技术漏洞
26	2021/6/23	Eleven Finance	ApeSwap	技术漏洞
27	2021/6/25	xWin Finance	PancakeSwap	操纵预言机
28	2021/7/2	XDXSwap	XDXSwap（Heco）	技术漏洞
29	2021/7/13	DeFiPie	PancakeSwap	重入攻击
30	2021/7/14	ApeRocket	PancakeSwap	技术漏洞
31	2021/7/14	ApeRocket	AAVE（Polygon）	技术漏洞
32	2021/7/16	Swamp.Finance	PancakeSwap	技术漏洞
33	2021/7/17	PancakeBunny	AAVE（Polygon）	技术漏洞
34	2021/7/18	Array.Finace	AAVE	技术漏洞
35	2021/8/4	Popsicle Finance	AAVE	技术漏洞
36	2021/8/4	Wault.Finance	PancakeSwap	技术漏洞
37	2021/8/17	XSURGE	PancakeSwap	重入攻击
38	2021/8/25	Dot.Finance	PancakeSwap	技术漏洞
39	2021/8/30	Cream Finance	Uniswap V2	重入攻击
40	2021/9/12	Zabu Finance	Pangolin	技术漏洞
41	2021/9/15	NowSwap	NowSwap	技术漏洞
42	2021/10/2	Twindex	Twindex	技术漏洞
43	2021/10/2	AutoShark	PancakeSwap	操纵预言机
44	2021/10/6	MY FARM PET	PancakeSwap	操纵预言机
45	2021/10/15	Indexed Finance	SushiSwap	技术漏洞
46	2021/10/20	PankeHunny	PancakeSwap	操纵预言机

SharkTeam reminds you to be vigilant when getting involved in blockchain projects, choose more stable, safer, and complete multiple rounds of auditing public chains and projects. You must not put your assets at risk and become hackers. Cash machine. As the project party, the security of smart contracts is vital to the safety of users' property! The blockchain project party should cooperate with a professional security audit company to conduct multiple rounds of audits to avoid status and calculation errors in the contract, and provide guarantees for the security of users' digital assets and the security of the project itself.

As a leading blockchain security service team, SharkTeam provides developers with smart contract audit services. The smart contract audit service consists of manual audit and automated audit to meet the needs of different customers. It exclusively implements nearly two hundred audit contents covering the four aspects of high-level language layer, virtual machine layer, blockchain layer, and business logic layer, fully guaranteeing smart contracts Safety.


SharkTeam
About
SharkTeam focus on smart contract security, composed of members with many years of practical experience in front-line cyber security and blockchain. We are proficient in the underlying principles of blockchain and smart contract, and has perfect capabilities in blockchain vulnerability mining and smart contract audit. We can provide comprehensive threat modeling, smart contract audit and emergency response services, SharkTeam has helped several well-known blockchain projects find and fix security vulnerabilities, and is committed to protecting the security of users' digital assets and privacy.
Security Vulnerability
Ethererum Virtual Machine (EVM) Layer
Business-Logic Layer
Nearly 200 Exclusive coverage
High-level Language Layer
Blockchain Layer
Security Service
7*24h online
Automated audit
Automated scanning
Exclusive coverage
High precision
Manual audit service
VIP Security Audit Service
VIP compliance audit service
Emergency response and contract customization
Partner
OKEX
Huobi
Twitter: @sharkteamorg
Telegram: https://t.me/sharkteamorg

SharkTeam

In Math, We Trust !

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg