Check Point Research detects Vulnerability in the Rarible NFT Marketplace, Preventing Risk of Account Takeover and Cryptocurrency Theft

April 14, 2022

14/04/2022

Research by: Roman Zaikin, Dikla Barda & Oded Vanunu

Highlights:

- Check Point Research identifies a vulnerability within the Rarible NFT Marketplace that allows attackers to take over cryptocurrency wallets
- By luring victims to click on a malicious NFT, an attacker can take full control of the victim's crypto wallet to steal funds
- CPR immediately reported this flaw to Rarible, which acknowledged and installed a fix
- CPR urges users to remain aware and offers preventive actions

Background and responsible disclosure

Rarible is an NFT marketplace that enables users to create, buy, and sell digital NFT art like photographs, games, and memes. The company reported over $273 million trading volume in 2021, and more than 2.1 million users, making Rarible one of the biggest NFT marketplaces in the world as they also supports three blockchains with over 400,000 NFT's minted. In addition, Rarible provides NFT creators with a large earning potential through royalties, as these creators can earn up to 50% in royalties whenever someone resells their NFT on the secondary market. CPR researchers found a design flaw within the marketplace that can potentially allow attackers takeover users' cryptocurrency wallets, by luring them to click on a malicious NFT, and take full control over their account, including the funds in it. CPR immediately alerted Rarible about this potential risk, who then collaborated with our researchers, acknowledged the flaw and installed a fix.

Technical Details:

Non-Fungible Token has a standard (EIP-721), which provides basic functionality to track and transfer NFTs. This standard has a function called setApprovalForAll.

This function basically designates who is authorized to control all your tokens/NFTs, which is mainly created for 3rd parties like Rarible/OpenSea, etc. to control the NFT/tokens on behalf of the users.

Figure 1: SetApprovalForAll example

This function is very dangerous by design because this may allow anyone to control your NFTs if you get tricked into signing it. It's not always clear to users exactly what permissions they are giving by signing a transaction. Most of the time, the victim assumes these are regular transactions when in fact, they were giving control over their own NFTs.

Figure 2:Metamask SetApprovalForAll transaction

Attackers use this kind of transaction usually in phishing attacks, but when it comes from the NFT marketplace itself, it is much more dangerous. We looked at the Rarible NFT marketplace which allows anyone to create and sell art. Art can be anything that ends with the following extensions: PNG, GIF, SVG, MP4, WEBM, MP3. Max size: 100 MB.

CPR decided to check the outcome of creating malicious art that contains code in it, for example, an SVG image. We created a simple SVG file and uploaded it with a simple payload, which looked like this:

Link to the art:

https://rarible.com/token/0xc9154424B823b10579895cCBE442d41b9Abd96Ed:95940970306686048929819095111797470789103351265739090847752668988066603466762?tab=details

By clicking on the art and opening it in another tab, or by pressing on the IPFS link from the drop-down, the JavaScript code will be executed.

What so great about wallet transactions is it doesn't have to run under the same domain, so we don't need any private information such as cookies, or sessions, all the victim needs is a wallet and the attacker will use the JSON-RPC to abuse it Our payload first checks what NFTs the victim has, by using Ethereum API "tokennfttx":

Then we loop through all the NFTs, sending the setApprovalForAll transaction to the wallet.

In this example, we just focused on the BoredApeClub Contract:

By clicking on the confirm button, the attacker will have full access to all the NFTs the victim has under the desired contract ,which is full access to all the victim's BoredApeClub NFTs:

The attacker can now transfer all the NFTs to his account by using the transferFrom action on the boardApeClub contract because the victim has 'allowed' him to do so:

This same attack vector was used in the first week of April, when an attacker tricked Jay Chou, a famous Taiwanese singer, songwriter, rapper, record producer, and actor. To click on a setApprovalForAll request which granted the attacker full access to Chou's BoardAppeNFT's 3738 NFT, this transaction can be seen here:
https://etherscan.io/tx/0xb8a5c47dad2637b98b09e4cf97d2b7ff2ee08e344af70ae4cf2ba0e725651bb0

After Chou submitted the request and granted the attacker access to the NFT, the attacker transferred the NFT to the attacker's own wallet 0xe34f004bdef6f069b92dc299587d6c8a731072da, and later Sold the NFT on the marketplace for $500,000.

NFT users should be aware that there are various wallet requests — some of them are used just to connect the wallet, but others may provide full access to their NFTs and Tokens.

How to protect yourself?

- CPR recommends being careful and aware whenever receiving requests to sign any link within the Rarible marketplace, or any other marketplace.
- Prior to approving a request, users should carefully review what is being requested, and consider whether the request seems abnormal or suspicious.
- If there are any doubts, users are advised to reject the request and examine it further before providing any kind of authorization.
- Users are advised to review and revoke token approvals under this link: https://etherscan.io/tokenapprovalchecker.

Conclusions:

Blockchain innovation is fast-underway and NFTs are here to stay. Given the sheer pace of innovation, there is an inherent challenge in securely integrating software applications and crypto markets. Threat actors know they have an open window right now to take advantage of, with consumer adoption spiking, while security measures in this space still needs to catch up. The cyber security community must step up to help pioneering blockchain technologies secure the crypto assets of consumers.