pNetwork Post Mortem: pBTC-on-BSC Exploit

pNetwork Team · Follow
Published in pNetwork · 7 min read · Sep 21, 2021

42 2

Foreword: All funds in bridges other than pBTC-on-BSC are safe. All bridges other than pBTC-on-BSC are not at risk.

Let us start by saying how sorry we are about the incident and by reassuring you that we have stopped the exploit and are now working on restoring operations for the entire system. We want to reiterate that the team is committed to the project long-term and we will use this experience to learn and come back stronger.

We are working on several fronts to find solutions that prioritise recouping value for pBTC-on-BSC holders while maintaining value on the project for the pNetwork community.

If you are interested in reaching out to us directly or in receiving real-time updates, you can join our Telegram group.

What happened?

On September 19th, 2021 at 5:20pm UTC time, the pNetwork system was attacked by a hacker who performed the offensive against multiple pTokens bridges. However, the exploit was only successful on the pBTC-on-BSC cross-chain bridge, which bridge was exploited and 277 BTC, stolen from the pBTC-on-BSC collateral. The first exploit transaction is:

https://bscscan.com/tx/0x0eb55e02bc39ec1d2d2e911eca7dcca54e74841b53412c078185e43c5a2a5551

While they tried to attack pBTC-on-BSC, TLOS-on-BSC, PNT-on-BSC, pBTC-on-ETH, TLOS-on-ETH, pSAFEMOON-on-ETH, they were able to steal the BTC collateral for the pBTC-on-BSC bridge only.

We want to reassure everyone that pBTC-on-BSC is the only bridge that was successfully attacked. **All other bridges such as pBTC-on-ETH or pBTC-on-EOS were not affected.** The funds for all bridges other than pBTC-on-BSC are safe.

This is the first time pNetwork has been exploited directly.

How did it happen? Technical explanation

The attacker funded their 0x2bf5693dd3a5cea1139c4510fdce120cf042c934 account by withdrawing BNB tokens from Binance (https://bscscan.com/tx/0x224b9ee27e10512fded6659a743fd6df92d482ad679685 1c71127e5049e7bbd88) and then used the account to deploy a set of smart contracts specifically crafted to abuse the peg-out instructions the pNetwork nodes look for.

These smart contracts created a series of event logs: one of those being a legit peg-out request, while the others were faulty peg-out requests emitted by the attacker's smart contracts rather than from the pToken ones.

Due to a bug in the section of the Rust code in charge of extracting these log events, both the legitimate and the faulty logs were extracted and erroneously processed.

The attacker proceeded to move the stolen BTC to a list of addresses that are still holding the funds at the time of writing.

Below is a list of addresses that are known to belong to the attacker:

- the Telos account "testacct1234"
- the Ethereum/BSC address 0xD27b89B384EF33EB17F6D98AFD9A47332543664
- the Ethereum/BSC address 0x2bf5693dd3a5cea1139c4510fdce120cf042c934
- the following BTC addresses: LINK

What happened after?

The technical team was prompt to detect a potentially malicious operation and intervene. The attack started at 5:20pm UTC, the misbehaviour was first noticed at 5:33pm UTC, at 5:40pm UTC the main bridges were stopped, by 5:59pm all the bridges were stopped. The team started an investigation and identified the bug that was exploited — the bridges remained temporarily suspended while a further investigation and fixing of the root cause were ongoing.

On the technical side, we identified the bug and worked on a fix with the support of our usual external auditing firm. A fix was implemented for the exploited pBTC-on-BSC bridge at 7:45pm UTC time.

In the meantime, it was our top priority to make sure funds on all other bridges were secure.

We are reviewing in detail all of the bridges for the same and similar potential exploits before re-activating them. As soon as it is confirmed they are safe, we are gradually reactivating the bridges with extra security measures in place. Already reactivated bridges are pBTC-on-EOS, pBTC-on-Telos, pLTC-on-EOS, pUOS-on-Ultra — none of which were affected by the hack.

Whilst we have confirmed already that no bridge other than pBTC-on-BSC was affected by the attack, the gradual reactivation of the bridges allows for additional security reviews to be performed before going back to normal operations.

We are adding additional security measures on the bridges as we reactivate them (more on this in the risk management section). Currently, we are also doing some extra checks on the transactions before they are broadcasted — this is not necessary, but something we are temporarily doing to be on the safe side andextra cautious.

On the attacker tracking side, at 6:40pm UTC we identified and collected the BTC addresses the hacker used for the attack and we reported them to exchanges right after the hack. This is useful so that exchanges can intervene on the funds in case they are moved on one of those platforms, since they are now all blacklisted.

The stolen BTC are currently on the hacker BTC addresses and have not been moved since the hack.

We have offered the attacker a bug bounty of $1,500,000 if they return the funds (which was also communicated onchain with this tx: https://bscscan.com/tx/0x5937ba4b846df4ae2119ff674716dbeb2b9dabd264eec2f7c7b3f1b2588900ecb). We have not received an answer yet. To the black hat hacker: the offer still stands.

In the meantime, we are continuing to follow the traces the attacker has left, along with the collaboration of some external parties. We are really thankful for everyone in the community who is helping with this.

From an ecosystem perspective, we reached out directly to both exchanges and projects we work with to inform them of the situation. We are really grateful for the support we received.

Who is affected?

The exploit affected the pBTC-on-BSC bridge only. **Anyone holding any other pTokens was not affected.**

If you are currently holding pBTC-on-BSC, then you are affected and we are working to find a solution that compensates you for the value lost as a result of the hack while maintaining value on the project for the pNetwork community.

If you did hold pBTC-on-BSC in the past and exchanged them for another asset (so you are currently not holding pBTC-on-BSC), then you are not among the people part of the compensation plan.

What will happen next?

As a community, we have long-term goals for pNetwork and we will use this exploit to improve and come back stronger. pNetwork will continue to build and innovate prioritising security of its users.

From a risk management perspective, we are implementing additional security measures to the system. We are adding additional checks on the signed transactions to be performed before they are broadcasted. Plus, we are implementing additional checks on the pNetwork system in reference to transactions processed so as to trigger protective actions when specific situations happen. These will be enabled permanently.

Following the initial security audit of the protocol, back in September 2020 the project had introduced a continuous security auditing process in collaboration with Cryptonics Consulting, that will continue being used as it provides continuous monitoring and external reviews of the codebase as it evolves. While the current situation didn't benefit from it, we feel like this activity is an important piece of the puzzle that contributes positively to the overall security and advancements of the protocol.

We are in touch with well-known security auditing firms so as to obtain additional audits of the entire codebase. We expect this activity to be a recurring task whose outputs will continue being shared with the community.

We are working on introducing a bug bounty programme for white hat hackers to contribute to the security of the system. The open-source nature of the pNetwork codebase makes it possible for white hat hackers to identify potential vulnerabilities in the code and securely report without impacting users in exchange for an economic benefit.

Moving forward, it is a top priority for us to find solutions that compensate current pBTC-on-BSC holders for the value lost as a result of the hack while maintaining value on the project for the pNetwork community.

We have offered the attacker a bug bounty of $1,500,000 if they return the funds. We have not received an answer yet. The funds stolen are still on their BTC address and have not been moved since the hack. We will wait a few more days to give the attacker the possibility to come forward before moving forward with defining the exact steps of a compensation plan.

The steps forward are ultimately a community decision, not a team decision. It is our intention to preserve long-term value in pNetwork and we feel like a critical component to do that is enabling the parties involved to share their feedback and their suggestions.

The team will continue updating the community as the entire system gets back to normal operations.

In the meantime, should the attacker not return the funds, proposals on the steps-forward for compensating current pBTC-on-BSC holders for the value lost as a result of the hack will be shared for everyone's review. There are a range of possible solutions, one for example is that the pNetwork has experienced organic growth over the past few months resulting in an increase of both Total Value Locked and cross-chain volumes therefore producing positive returns for the project — mostly in BTC — that could be partially redirected to compensating users. Of paramount importance though is that that the road ahead for the project is a *shared* decision of the pNetwork community. Proposals will be opened in the pNetwork DAO to give PNT token holders the possibility to vote and contribute in finding a balanced solution for all parties involved. More details on this to follow.

***To conclude,** we are committed to making this right for those negatively affected by the event. We are committed to the industry and continue building innovative products. We want to thank everyone who supported us during this difficult time and are committed to going back stronger together.*

The pNetwork team