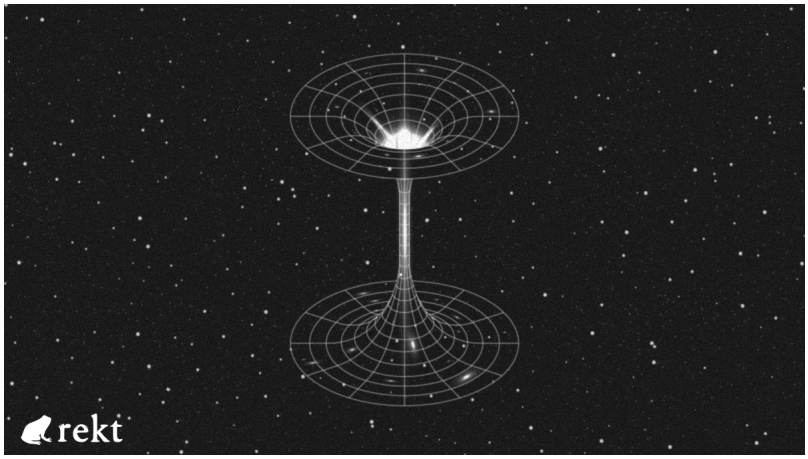
WORMHOLE - REKT

Thursday, February 3, 2022

Wormhole (/?tag=Wormhole) - Solana (/?tag=Solana) - REKT (/?tag=REKT)

read this article also in:

de (/de/wormhole-rekt/) - en (/wormhole-rekt/) - es (/es/wormhole-rekt/) - fr (/fr/wormhole-rekt/) - ko (/ko/wormhole-rekt/) - ru (/ru/wormhole-rekt/) - tr (/tr/wormhole-rekt/) - zh (/zh/wormhole-rekt/)



Wormhole had a loophole…

A hacker distorted the fabric of Solana's space-time, netting $326M in the process.

In the second bridge exploit in less than a week (https://rekt.news/qubit-rekt/), Solana's Wormhole goes straight to 2nd place on our leaderboard (https://rekt.news/leaderboard/).

Minutes after samczsun (https://rekt.news/qubit-rekt/) pointed out that there was a problem, the Wormhole team stated (https://rekt.news/leaderboard/) that the network was simply *"down for maintenance"* whilst investigating a *"potential exploit"*.

The exploit was later addressed (https://twitter.com/samczsun/status/1488974372756987906) directly, with a bold promise to restore the funds:

> *The wormhole network was exploited for 120k wETH. ETH will be added over the next hours to ensure wETH is backed 1:1.*

Less than 24 hours later, and the backing has just been restored (https://twitter.com/wormholecrypto/status/1489232008521859079).

Where did Wormhole find $326M?

Credit: @samczsun (https://twitter.com/samczsun/status/1489044939732406275?s=20&t=_rQJze06-VjgQls6hu73wA), @gf_256 (https://twitter.com/gf_256), @ret2jazzy (https://twitter.com/ret2jazzy), @kelvinfichter (https://twitter.com/kelvinfichter)

Attacker address: 0x629e7da20197a5429d30da36e77d06cdf796b71a (https://twitter.com/samczsun/status/1489044939732406275?s=20&t=_rQJze06-VjgQls6hu73wA)

The Wormhole, Solana's bridge, was manipulated into crediting 120k ETH as having been deposited on Ethereum, allowing for the hacker to mint the equivalent in wrapped whETH *(Wormhole ETH)* on Solana.

1: Using a *SignatureSet* created in a previous transaction (https://solscan.io/tx/5fKWY7XyW6PTzjviTDvCTpsqgfoGAAqUs1mC6w4DZm25Ppw7fX7aWDmrnkknewyZ81qMSix3c18ZuvjoZUF34tpa), the attacker was first able to bypass Wormhole's 'guardians' - (put in place to verify transfers between chains), and call *'verify_signatures (https://solscan.io/tx/25Zu1L2Q9uk998d5GMnX43t9u9eVBKvbVtgHndkc2GmUFed8Pu73LGW6hiDsmGXHykKUTLkvUdh4yXPdL3Jo4wVS)'* on the main bridge.

2: The *'verify_signatures'* function of the contract then delegates the actual verification of the *'SignatureSet'* to a separate Secp256k1 program. Due to a discrepancy between 'solana_program::sysvar::instructions' (a precompile of sorts) and the 'solana_program' Wormhole was using, the contract didn't correctly verify the address being provided, and the attacker was able to provide an address containing just 0.1 Eth.

3: Using an account created hours earlier with a single serialised instruction corresponding to the Sep256k1 contract, the attacker (https://etherscan.io/address/0x629e7da20197a5429d30da36e77d06cdf796b71a#internaltx) was able to fake the *'SignatureSet'*, call *'complete_wrapped'* and fraudulently mint (https://solscan.io/tx/2zCz2GgSoSS68eNJENWrYB48dMM1zmH8SZkgYneVDv2G4gRsVfwu5rNXtK5BKFxn7fSqX9BvrBc1rdPAeBEcD6Es) 120k whETH on Solana using VAA verification that had been created in a previous transaction. (https://solscan.io/tx/2SohoVoPDSdzgsGCgKQPByKQkLAXHrYmvtE7EEqwKi3qUBTGDDJ7DcfYS7YJC2f8xwKVVa6SFUpH5MZ5xcyn1BCK)

4: 93,750 ETH was bridged back to Ethereum over the course of 3 transactions, (one (https://etherscan.io/address/0x629e7da20197a5429d30da36e77d06cdf796b71a#internaltx), two (https://etherscan.io/tx/0xd31b155e259a403ebe69831fae0ec2b4bd33dfa090c43b605a57d5c72c4fbbc7), three (https://etherscan.io/tx/0xacd309b02e4b533484d148de9ab0adf367ed4e70ed751d1ff036152dc3bc0479)) where it still remains in the hacker's wallet (https://solscan.io/tx/2zCz2GgSoSS68eNJENWrYB48dMM1zmH8SZkgYneVDv2G4gRsVfwu5rNXtK5BKFxn7fSqX9BvrBc1rdPAeBEcD6Es). The remaining ~36k whETH were liquidated on Solana into USDC and SOL.

An on-chain message (https://etherscan.io/tx/0x2d8b7901bff18ae6abe1a50aebe44b70559f39ff357b21340843d368b9486859) was sent to the hacker from Certus One, the team behind the Wormhole bridge:

> *This is the Wormhole Deployer:*
>
> *We noticed you were able to exploit the Solana VAA verification and mint tokens. We'd like to offer you a whitehat agreement, and present you a bug bounty of $10 million for exploit details, and returning the wETH you've minted. You can reach out to us at contact@certus.one (mailto:contact@certus.one).*

A $10M bug bounty is the biggest we've seen.

Keep your innocence, plus $10M, or go on the run with $326M.

Which would you choose?

As Wormhole have yet to receive any response to their offer, it seems the attacker has chosen the criminal route…

We spoke to the founders of Wormhole, and asked how they managed to replace so much ETH so quickly.

After waiting for some time, they would only tell us that they are currently writing a more detailed incident report.

It's not been a good start to the year for Solana.

The last few months has seen the network experience a number of outages and disruptions. However, in the recent January crash, users were unable (https://twitter.com/solendprotocol/status/1485315186797936646) to top up their collateral and avoid liquidation, with oracle issues (https://twitter.com/solendprotocol/status/1485315192716083202) leading to further erroneous liquidations.

That being said, Solana is not yet the battle-hardened network that Ethereum has grown to be. Every exploit, for all the damage it does, offers a lesson for how to secure an evolving ecosystem. Newer L1s are thrown into the deep end, into a world of veteran exploiters where they will either sink or learn to swim.

Given the seriousness of this incident, along with the Qubit exploit (https://rekt.news/qubit-rekt/) last week and last summer's mammoth attack on Poly Network (https://rekt.news/polynetwork-rekt/), Vitalik Buterin seems to have been proven right about his recent security concerns (https://twitter.com/vitalikbuterin/status/1479501366192132099) around cross-chain protocols.

In the race across the cryptoverse to reach experimental and more lucrative opportunities, many are willing to trust in newer tech. But when one of these gateways fails, the damage done can be immense.

It remains to be seen whether the future of DeFi will be cross-chain or 'multi-chain', but either way, the journey there will be long and dangerous.

REKT serves as a public platform for anonymous authors, we take no responsibility for the views or content hosted on REKT.

donate (ETH / ERC20): 0x3C5c2F4bCeC51a36494682f91Dbc6cA7c63B514C (https://etherscan.io/address/0x3C5c2F4bCeC51a36494682f91Dbc6cA7c63B514C)

disclaimer:

REKT is not responsible or liable in any manner for any Content posted on our Website or in connection with our Services, whether posted or caused by ANON Author of our Website, or by REKT. Although we provide rules for Anon Author conduct and postings, we do not control and are not responsible for what Anon Author post, transmit or share on our Website or Services, and are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content you may encounter on our Website or Services. REKT is not responsible for the conduct, whether online or offline, of any user of our Website or Services.

you might also like...

CASHIO - REKT (/CASHIO-REKT/)

03/23/2022

Cashio (/[slug]/?tag=Cashio) - REKT (/[slug]/?tag=REKT) - Solana (/[slug]/?tag=Solana)

$48M CASHed out. The latest leaderboard entry comes from the Solana network, where an anonymous attacker used an infinite mint to make Cashio print faster than the Fed.

MORE (/cashio-rekt/)

SPOTLIGHT ON SOLANA (/SPOTLIGHT-ON-SOLANA/)

09/13/2021

Solana (/[slug]/?tag=Solana) - Spotlight (/[slug]/?tag=Spotlight)

Was that Solana Summer? These cheaper, faster, centralised chains put the Ethereum "community" to the test. But are their claims accurate?

MORE (/spotlight-on-solana/)

INVERSE FINANCE - REKT (/INVERSE-FINANCE-REKT/)

04/02/2022

Inverse Finance (/[slug]/?tag=Inverse+Finance) - REKT (/[slug]/?tag=REKT)

Inverse Finance got flipped for ~$15M. A professionally executed hack allowed an anonymous actor to manipulate the price of INV and help themself to an exclusive deal from the ETH based lending protocol.

MORE (/inverse-finance-rekt/)

SUBSCRIBE

Hopium (https://www.youtube.com/watch?v=1175BnBuFgE) | Opensea (https://opensea.io/collection/rekt-news-hacks-hopium)

(http://eepurl.com/hd4HkD)