P2P Storms

Report By **Jacob Gadikian**
Research by **Khanh Nguyen, Andres Monty,** and **@ctrl_felix**
Data Support by **Jerry Chong** and **Clemens Scapataetti**

9/21/2023

 contact@notional.ventures

 notional.ventures

 github.com/notional-labs

This document outlines a liveness vulnerability on 100% of tendermint and comet networks

Note: this document is undergoing substantial revision, constantly. Some parts may not match other parts. This document corresponds to this GitHub repo:

GitHub.com/notional-labs/spammy

The vulnerability

In networks with sufficiently complex p2p networks, full 20mb blocks and a full mempool yield a condition where chains stop producing blocks reliably.
This has been seen on the following mainnets in this order:

- Sentinel in 2021
- Luna Classic in 2022
- Stride in 2023

Having high or higher gas fees increases the cost of the attack, but short positions should easily be able to make the attack economically viable.

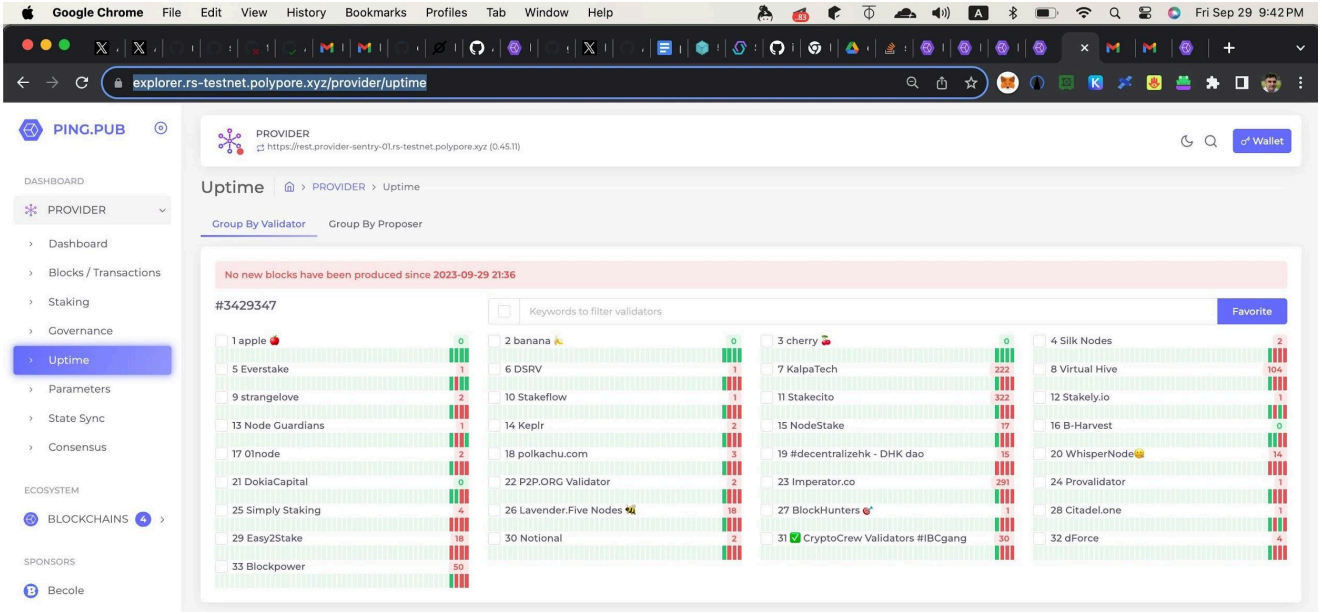
Especially vulnerable

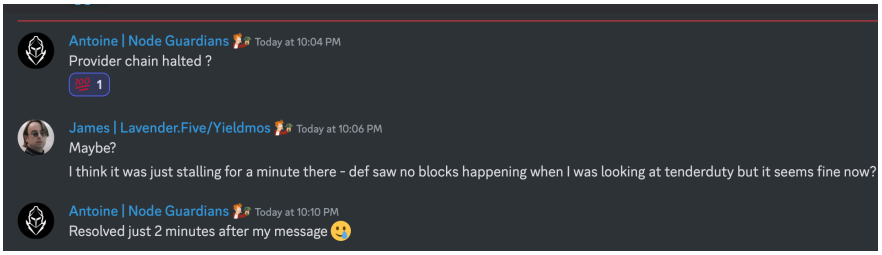
- **Juno**
  - https://github.com/CosmosContracts/juno/blob/b03500a3f4d7cea9d6d8de11e0a63c6d92502dc2/app/app.go#L491
- **Cosmos Hub**
  - https://github.com/cosmos/gaia/blob/a4eb27a3831340c9505653012c8e3f204a90961d/x/globalfee/types/params.go#L24-L33
- **Noble**
  - https://github.com/strangelove-ventures/noble/blob/fcb702cda3c8fcc7982a25ac78eb3723edd45f19/x/globalfee/types/params.go#L22
- **Quasar**
  - Valeyo describes a safety mechanism that protects funds in event of a chain halt
- **Sommelier**
  - User funds depend on liveness
- **Umee**
  - User funds depend on liveness
- **Mars**

Vulnerable

Every cosmos chain is vulnerable to this, provided that the attacker is willing to pay for downtime.

Proof that every chain is vulnerable, provided attacker is willing to pay for downtime:





Attack scenarios

“The halt and short” - Suppose that the cosmos hub immediately ceases block production, or cannot accept transactions properly due to a flooded mempool, and produces a block every 80 seconds. Note, I think that the attack is scalable beyond what was seen on Stride and Sentinel, and that it could be used to produce a full halt condition, though when the spamming stopped it is likely that the chain would resume producing blocks as normal.

1. Attacker a jerk with a moderate amount of capital
2. Attacker wants to make money on a 30x short
3. Attacker floods the hub with invalid client update transactions or similar
4. Attacker gets the hub to make 80 second blocks like happened to stride
5. Attacker and co-conspirators flood the x.com with the fact that this is happening
6. Prices fall
7. really big profits

“The Explorer” - I think this is what happened on Sentinel and Stride, but in both cases it is possible that the attacker found ways to profit, since the networks were forced into very poor operational state.

1. Attacker is a pentester
2. Attacker wants to learn about an issue she has a hypothesis about
3. Attacker tests the attack but only in ways that do not cost them money
4. Attacker floods network with invalid client update transactions

Stride - Aug 14, 2023 to Aug 19, 2023

Let's run through the symptoms:

- High block time
- High rate of proposal failure
- Nodes unable to get the whole block
- Blocks filled with invalid client updates
- Full blocks containing 336 block parts
- Full Mempool
- Block size of about 20 megabytes
- Bandwidth consumption of 500mbps in both directions
- Range security mentions that blocks were full of invalid client updates

Now, let's go through the fix:

- Require nonzero gas

But wait, this happened before?

Luna Classic in May 2022

Report:
https://github.com/notional-labs/notional/blob/master/incidents/WTF%20HAPPENED%20TO%20TERRA.pdf

The attack on Luna classic showed the exact same situation – without invalid client updates – as Stride and Sentinel. Basically, blocks (20mb each) filled up and the mempool hit full capacity. Chain liveness and use ability to transact was impacted, resulting in liquidations on the Anchor smart contract.

As Terra Classic became unstable:

- Block production slowed
- New transactions could not get into blocks
- Proposals failed
- Validators could not get the complete block to sign
- Bandwidth consumption exceeded what validators could handle

Unfortunately, we never were able to remedy the situation on terra classic. A p2p flood was used to enhance the effectiveness of the financial attack against UST, and users ultimately lost billions of dollars. The Columbus-5 network still has not regained its former value, and I suggest that it is possible that the financial attack alone may not have been enough to push the network over.

The following services were impacted from my observations:

- Chain liveness
- Ability for users to transact

In a 1:1 interview about one week before his incarceration, Do Kwon explained to me (Jacob Gadikian) that the http endpoints were also attacked during this time. He felt that this was to prevent users from being able to adjust their positions so the attacker could profit from liquidations. Luna classic blocks had 600+ transactions in them at any of the peak times for the attack.

Sentinel in Fall 2021

It was the exact same issue as on Stride, full 20mb blocks full of invalid client updates. The issue was diagnosed by Khanh Nguyen from Notional. A hacker one report was created. Turnaround time was 18 days. Payment was nil.

Let's run through the symptoms:

- High block time
- High rate of proposal failure
- Nodes unable to get the whole block
- Blocks filled with invalid client updates
- Full blocks containing 336 block parts
- Block size of about 20 megabytes
- Bandwidth consumption of 500mbps in both directions, max observed was 1gbps
- Range security mentions that blocks were full of invalid client updates

Now, let’s go through the fix:

- Require nonzero gas

Is the fix fix?

I think not. In the sentinel and Stride cases the attacker was not willing to pay gas. In the Luna Classic case, the attacker did pay gas and the attack was successful.

Documentation:

- https://github.com/notional-labs/Tendermint_issues/blob/main/Attack_on_sentinel.md
    - Blocks full of invalid client updates
- https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:c14b2605-3497-381a-870e-510b92e33f75
    - Turnaround time was 18 days.
    - Payment was nil.
    - This is our 3rd related report.
- Attacker account
    - https://www.mintscan.io/sentinel/accounts/sent1v5amm7pkk0mwccsly0pv6ggf0tfa6x4x4x4jkr

Mitigation

In addition to fixes made by Sergio and Ethan Bunchman from informal, we should reduce the default maximum block size. 20mb blocks are simply extraordinary and are not something we need to support.

- Don't use sentry node architecture
    - In order to maximize connectivity between validators
-
- Have validators connect directly to one another over vpns that they build following the trust graphs that they have established between one another
    - Maximizing connectivity between validators can fully mitigate this
- Discuss questions relating to gas for client update transactions
    - Get a link to code demonstrating this?
        - https://github.com/cosmos/gaia/blob/a4eb27a3831340c9505653012c8e3f204a90961d/x/globalfee/types/params.go#L24-L33
        - The hub is super vulnerable to this specific attack

Difficulty surrounding replication on a testnet

Cosmos hub testnet has about 100ish nodes.

Let's make the inaccurate assumption that we are dealing with a fully connected graph and that every peer will broadcast to every other peer, when they've got a block proposal. Reality is more complex:

20mb block * 100 peers = 2gb
However, then those peers rebroadcast to one another, yielding 200gb

And this is why networks would go down.

Cosmos hub mainnet has about 3500 nodes if we scan from a european datacenter.

20mb block * 100 peers = 2gb
2gb * 100 = 200gb
2gb * 100 = 200gb
2gb * 100 = 200gb
2gb * 100 = 200gb
2gb * 100 = 200gb
2gb * 100 = 200gb
2gb * 100 = 200gb

… and so on until we see that:

- It isn't clean 100 to 100
- Some nodes may have hundred of peers
- Some may have very few peers
- In any event the p2p network will certainly be overwhelmed fully* *

Cosmos hub mainnet has about 2352 nodes if we scan it from a laptop in Bali

Same as above

Conclusion to this section

Testing this attack on a testnet might reproduce a bandwidth issue but actual reproduction of this issue likely requires a network with a mature, complex p2p network that features sentry node architecture. And that's mainnets.

Teams informed.

Due to the fact that this attack will be far more severe on the mainnet than a testnet, and that the hub is imminently vulnerable, I reached out directly to the necessary teams and look forward to working with them on a solution to this issue.

- Informal
  - Slack
- IBC
  - Slack
- Quasar
  - Telegram

    - In person
- Stride
    - Slack
- Skip
    - Slack
- Iqlusion
    - Slack
- Range Security
    - Slack
- Neutron
    - Slack
- Notional
    - Slack
- Osmosis -
    - Dev via signal
    - Sunny via signal
- Allinbits
    - Carolyn and Adriana via signal
- Terraform Labs - MC and Mike via telegram
- Validator working group on spam per recommendations here
    - https://github.com/cometbft/cometbft/security/advisories/GHSA-hq58-p9mv-338c
- Amulet
    - Slack channel invite
    - Google docs invite to jessy@amulet.dev
    - Google docs invite to security@interchain.io
    - E-mail to security@interchain.io

Reproducing

First of all, I want to state that I think that the attack has been more than sufficiently reproduced, and that the sensible course of action is for cosmos networks to take the defensive actions mentioned in the mitigation section. Anyone with an archive node for Sentinel or Stride or Luna Classic can easily understand the full attacks in detail.

With that said, it seems that the ICF via Amulet requires reproduction to be paid a bounty, and well, we're going for the 2021 report. It was never paid and that irks us.

Easiest means of reproduction

- Find tendermint networks with sufficiently complex p2p networks
- Spam until the mempool is full

Please note that unlike whomever attacked stride, as a white-hat, I am not terribly interested in attacking a mainnet. Efforts to attack the cosmos hub testnet are underway, however.

Specific methods

NOTE: the methods listed below are likely non-exhaustive. For example, Terra Classic was flooded with contract transactions. The critical factors to perform this attack successfully are:

- large (20mb) blocks and a
- full mempool
- Sufficiently complex peer to peer network

Methods

- Banana King (known to work)
    - Oversized IBC transactions that are valid due to a lack of field length limitations in ibc, failure of constraints in cosmos-sdk and failure of maxtxbytes in comet.
- Client Update Spam (known to work)
    - Spam client updates until blocks are full, as seen on Sentinel and Stride
- Banana Client (will be tested in next 24h, expect it to work)
    - Use the lack of field length limitations in ibc to create client updates that are 1-20MB in size each
    - The banana client attack should have no cost on
        - Cosmos Hub
        - Noble
        - Juno

Info Needed to Reproduce

- A client update transaction from Stride during the attack

Tooling needed to reproduce

We're going to need client-spammer, which can be found at: (private repository)

https://github.com/notional-labs/spammy

And we are also going to need a fresh, local cosmos hub testnet node:

https://github.com/cosmos/gaia/pull/2745

Note, if you are performing the attack from a laptop in Bali, like I am, it may limit the effectiveness. For maximum effectiveness, it may be helpful to connect to tons and tons of peers.

Evidence of reproduction

HEIGHT	HASH	PROPOSER	TXS	TIME
3382614	FF9TpPWK2ZIckDnpVlsqst4erBdaQa+g1SHIqIjxEV0=	P2P.ORG Validator	0	10s ago
3382607	XmNWa448dK3CTyYpj0bzH1X+1WH8gHtRUUfp8NumeaA=	Node Guardians	0	1m ago
3382599	IiJTMacwFX8nUYG92WSzxLqS1H9A+gmFHJNwp8ugKfw=	cherry 🍒	25	2m ago
3382591	mmjV0IFsnyqaGT+432TiayXOW49lfQgIwUcv5pWOdIk=	apple 🍎	21	3m ago
3382572	NiU4940EHRQwcUqguIsqvi23scXR9H/clYLFDuy98RU=	KalpaTech	15	5m ago
3382565	7M90VC8RJyZKLeqf+XBQpHZufrmVQcTFZXK+zF9TmOc=	banana 🍌	25	6m ago

HEIGHT	HASH	PROPOSER	TXS	TIME
3382332	AB+FOBEUsDTFN90JD+xOLUNTHSZnaMtikoX4sfM+8r8=	banana 🍌	7	28s ago
3382328	q7kDjGvJ7d9Jsqy7UbV8NJFNZSzqhjnMIK+B2gCdQps=	banana 🍌	0	1m ago
3382318	SKmJaLPZfWqUwLTwV9fx/4wECcsV+4hZSIzSZOCDP8U=	apple 🍎	0	2m ago
3382308	OtLCIt5fXX2R3jJX+s9ukMjI3lXwy+2dOCZ8Dpmoj00=	Everstake	0	3m ago
3382298	/TY9GFkP7eBK2zwJK2udgKD7Ml/bva1jRQiZgNwaUPs=	banana 🍌	0	4m ago
3382290	ivO9CTRBEq/tsfviXUtmd1ckIjlemkh+99qlWnY38tI=	DokiaCapital	0	5m ago
3382280	h3FBQI5ZC6/hQ4GlYMaf9rleisLM7Y6tAPsVFI9z8n0=	#decentralizehk - DHK dao	0	6m ago
3382270	Qd12IqZgqpbDkxbt5tykgVQiICKzGrzkReJSmvrAsd4=	apple 🍎	0	7m ago
3382260	7qtISVIj3hdEM/coUfeNW+vpH5umQ6ceiEd9u9WNzgY=	banana 🍌	0	8m ago

State bloat implications

Client updates are not saved to state, just the most recent.

Stats and stuff

Discrete issues covered here (I think there are more)

1) txns are gossiped if out of gas allowing a free or low cost way to kill p2p

- Ibc transfer transactions aren't whitelisted on cosmos hub
- They were free on hub replicated security testnet
- These transactions can be made ineffective by setting gas to 0.0025uatom
- We should just hard-code the gas price 0.0025uatom (we already knew this) - Sept 2021

2) out of gas transactions are committed to the chain, allowing a low cost way to expand archive nodes to a non-viable size rapidly 288 GB per day, assuming a 6 second block time, however one of the other additional attack vectors is the ability to slow the block time via number one

Testing underway - 9/27/2023

3) banana king - IBC receiver fields aren't validated for their length

4) banana memo - The IBC memo field can be up to it seems 50 kBytes and you can use this to exploit numbers one and two

5) client update spam - already reported to ICF via hacker one in 2021. Spamming client updates is an effective way to harm a chain. This is especially harmful to the cosmos hub because the hub whitelists the client update transaction for fees so it has no fee

6) comet default block size - the default block size in CometBFT is too large to be viable, at 20mb. This should be reduced to between one and five megabytes.

7) lack of throttling or back pressure on peer-to-peer. Peer-to-peer can be observed consuming over a gigabit per second in these attack scenarios.

Specific threats on specific chains:

* Noble, Cosmos hub, and Juno all white list the client update transaction

* Some chains depend on liveness. Users can lose money if certain chains go down.

* chains with faster block times are more negatively impacted: SEI, evmos, Juno

https://monitor.polypore.xyz/d/rYdddlPWk/node-exporter-full?orgId=2&var-DS_PROMETHEUS=default&var-job=provider-1&var-node=provider-apple.rs-testnet.polypore.xyz:9100&var-diskdevices=%5Ba-z%5D%2B%7Cnvme%5B0-9%5D%2Bn%5B0-9%5D%2B&from=now-24h&to=now