FSAF-report

My report to the Swiss FASF on the activities of the Interchain Foundation.

I think that this information is also likely to benefit teams actively working in Cosmos.

If you have security issues, I strongly recommend that you go directly to Dev Ojha who is extremely accomplished, ethical, and wonderful. I cannot recommend that you contact the Interchain Foundation due to the risks that:

- You will be harasssed
- Your issue will not be handled
- You will incur economic losses due to your report

For the P2P storms issue in particular, I needed to "disclose by demonstration", working in conjunction with SEAL911, an security reporting body of last resort. I also needed to spend my company's money to make a legal threat to the interchain foundation, as they refused to remove my company's name from a provably inaccurate report they published concerning an issue involved in over $70,000,000,000 in economic losses.

Who are you?

I'm Jacob Anthony Gadikian. I've worked in Cosmos since about 2016, but I began to do full time work in the ecosystem in 2020. I am the CEO and founder of Notional Ventures, which used to run 45 validators in the cosmos ecosystem.

- I am a direct and general beneficiary of the ICF, as my validator nodes recieved delegations from them, although this is not noted in the ICF's public facing delegation documents, which have commits only from Informal Systems team members:
  - ICF Delegation Information
    - Authored by Informal Systems members
  - Notional recieved a delegation of over 800,000 atoms, and this yeilded revenue of around $60,000 a year.
- My company was elected as the security provider to the Cosmos Hub

As time has gone on, I have noticed that issues are becoming worse with reporting, instead of getting better.

I am also a security researcher whose work tends to focus on the interplay between systems in cryptocurrency, and has been categorically denied by the Interchain foundation, despite ample proof. I prefer to speak and act directly, so I am doing this in a public fashion, my report to the FASF is this repository. I will speak to the FASF only over Signal, other than the initial e-mail that I send them with this repository and my signal contact information.

I do fear retaliation, both personal and professional, and I believe that being direct about my complaint and publishing my complaint is the safest path forward for myself and my family.

I am aware that my colleagues fear retaliation, both personal and professional.

And I think we have good reason to be afraid.

That is why I mentioned that fear in Cosmos Hub Proposal 787: Formally request full financial transparency from Interchain Foundation, which I authored.

In fact, the only reason I'm making this report is because I think that it is less risky to speak now, and speak fully, than to simply walk away.

Incidents

Due to the fact that there have been exploits following several of my reports, it is hard for me to say if it is safe from a network security perspective to bring security issues to the Interchain Foundation.

Amulet And the Fee Market

Please see:

- Issue on the Cosmos hub relating to the discrepancy between Amulet standards and the hub
  - backed up

Amulet, the security contractor to the Interchain Foundation, changed their cosmos hub reporting policies after the submission of a bug report by Joe Bowman, to claim that the incident was not covered by their reporting policy.

Here is the Original Report

HackerOne, the reporting service selected by the ICF and Amulet, keeps the versioned changes of security reports made via HackerOne.

Here is a link to their versioned reporting policy, where it can be seen that changes were made only after the report.

It is notable that the Security reporting process described on the Cosmos hub does not match the one described by Amulet:

- Cosmos Hub Security Docs
- Amulet / HackerOne Security Docs
  - go to the section "a note on gaia"
  - Here is the versioned edition of the reporting standards for the hub:
    - We can clearly see that the standards were modified after the report was made, and that Amulet attempted to say that the security issue was somehow Skip's fault (Skip is the third party that made the fee market module)
    - At the time of the report, Joe Bowman tested Osmosis to see if the vulnerability was present there, but due to differences in how Osmosis integrated the fee market, it was not.
    - This was a cosmos hub issue.

Threats made (and carried out) towards ecosystem participants by Strangelove Ventures, funded by the ICF

I watched Jack Zampolin and others associated with Strangelove Ventures, the team currently leading the growth of IBC, describe various means to stop the growth of IBC via composable specifically. To date, Composable is the only team that has meaningfully grown the IBC network. Composable has built IBC clients for both Cosmos and Polkadot, and designed 08-Wasm, a client interface.

Proposal 104

Proposal 104

Proposal 104 selected my company, Notional, as the security provider to the Cosmos hub.

- https://github.com/cosmos/interchain-security/issues/852

P2P Storms

I have deeply documented p2p storms in many ways, and have included PDF files here that describe it. You can find those in the p2p-storms folder.

P2P Storms have been used to exploit Cosmos networks financially, including Luna Classic and Osmosis. The links contain information on both exploits. Here is the chronology of exploits:

- Game of Zones - 2020

All cosmos hub game of zones participants noted this issue, yet it was not investigated.

- Sentinel - 2021

The Report linked here references the precise set of issues present in p2p storms.

- Luna Classic - May 2022
- Stride - August 2023
- Osmosis - December 2024

Only the exploits on Luna and Osmosis were financially consequential, but it should be noted that a p2p storm is basically the ultimate form of deniable blockchain attack. Since the transactions used are valid, it is impossible to prove much about these incidents except that they occured and were financially consequential. Addressing this issue when it was first reported may have prevented or lessened the catastrophic impact of Luna's UST stablecoin

failure. Please note that this is not an argument that UST was in any way risk free, or a satisfactory product. Much greater care should have been used in its construction.

My reports predate any of the financial exploits, and date back to 2021.

- https://www.range.org/blog/levana-security-incident-in-depth-analysis

Banana King: Lack of field length limitations in ibc

Reports

- First reported by x.com/@ctrl_felix to the Interchain Foundation using their formal security reporitng process.
  - ignored
- Reported by x.com/@getcoldy to me
- Reported by me to ICF

….and totally ignored for years until I opened an issue on the topic in public:

- Lack of Field Length Limitations in IBC

Myself and other reporters avoided making any comments in public, althought an analyst later found the issue:

- Web3 Analyst

Later, I met Jessica in person and we discussed both Banana King and p2p Storms:

- Inteview with Jessica

The content of IBC messages that exhibited banana king surpasses any reasonable bounds:

- Example Banana King tx

Banana king could be used to execute p2p storms style attacks, and the window to execute banana king attacks was left open by the Interchain foundation despite multiple reports, in a similar manner to the issues in P2P storms itself, and the submission of an initial patch in 2022.

Banana king did not result in any financial losses, but many cosmos chains remain vulnerable to it today. Mainly banana king allows for attacks on timing.

IBC Version 3.0.0 and the cosmos hub

Use of deprecated module on cosmos hub, leading to an exploit of the cosmos hub that caused 30,000 ATOM of user funds to get stuck Contrary to repeated, totally false claims made by the Interchain Foundation, the cosmos hub has been successfully exploited, with financial consequence for users (inability to access funds). This happened two weeks after I reported to both ICF and Informal Systems that the Cosmos Hub was using an obsolente version of IBC that was tagged as `deprecated` because:

- It was subject to the `Dragonberry` vulnerability
- It allowed ICA channels to be created only by using the counterparty's module name, enabling an attacker to block the creation of the ICA channel.