FSAF Report

Executive Summary

This report is submitted to the Swiss Financial Supervisory Authority (FASF) to provide a comprehensive overview of the activities and concerns related to the Interchain Foundation (ICF) within the Cosmos ecosystem. The report outlines various incidents, security issues, and potential conflicts of interest that may impact the integrity and security of the Cosmos network. Additionally, it highlights personal experiences and observations regarding the handling of security reports and the subsequent repercussions faced by ecosystem participants.

Table of Contents

Introduction

The purpose of this report is to inform the Swiss Financial Supervisory Authority (FASF) about significant activities and concerns related to the Interchain Foundation (ICF) within the Cosmos ecosystem. The Cosmos network is a decentralized network of independent, scalable, and interoperable blockchains, and the ICF plays a pivotal role in its governance and development. This report aims to shed light on potential security vulnerabilities, conflicts of interest, and instances of retaliation that may affect the overall stability and trustworthiness of the Cosmos ecosystem.

A PDF version of this report is available here, which is automatically generated upon each update to this markdown document.

Personal Background and Affiliations

I am Jacob Anthony Gadikian, CEO and Founder of Notional Ventures. My involvement with the Cosmos ecosystem began in 2016, and I transitioned to full-time work within the ecosystem in 2020. Notional Ventures previously operated 45 validators within the Cosmos network.

- **Affiliations and Benefits:**
    - **Delegations:** Notional Ventures received delegations totaling over 800,000 ATOMs from the ICF. These delegations generated approximately $60,000 in annual revenue. This financial relationship is not reflected in the ICF's public delegation records, which only list contributions from Informal Systems team members.
        * ICF Delegation Information
    - **Security Provider:** My company was elected as the security provider to the Cosmos Hub through Proposal 104.

While my involvement has provided valuable insights into the ecosystem, it is important to acknowledge potential conflicts of interest and strive for transparency to maintain trust and objectivity in reporting.

Summary of Incidents

Amulet and the Fee Market

Overview: Amulet, the security contractor for the ICF, altered the Cosmos Hub's reporting policies following a bug report submitted by Joe Bowman. The modification aimed to exclude the reported incident from their policy coverage.

Details: - **Issue Reference:** - Cosmos Hub Issue #3319 - Backup Documentation - **Original Report:** Fee Market Bug Report - **Reporting Platform:** HackerOne - **Policy Changes:** The security reporting policy was updated post-report submission, as detailed in the Versioned Reporting Policy.

Concerns: - **Policy Inconsistency:** The security reporting processes outlined in the Cosmos Hub documentation (Cosmos Hub Security Docs) differ from those implemented by Amulet (Amulet/HackerOne Security Docs), potentially leading to confusion and inadequate handling of security issues.

Threats by Strangelove Ventures

Overview: Strangelove Ventures, funded by the ICF, has engaged in actions that may hinder the growth of the Inter-Blockchain Communication (IBC) network, specifically targeting the Composable team, which has significantly contributed to IBC development.

Details: - **Key Figures:** Jack Zampolin and team members of Strangelove Ventures. - **Actions Taken:** - Proposed deploying Composable's Polkadot client code on alternative platforms (Juno or Noble) to delay its market release. - This strategy, termed "business stabby," led to a chain upgrade by Juno and subsequent feature promotions (Juno Network Announcement).

Concerns: - **Funding and Influence:** The ICF's financial support for Strangelove Ventures through consulting contracts may indicate a conflict of interest, as ongoing funding persists despite potential misalignments with ecosystem growth objectives.

Proposal 104

Overview: Proposal 104 resulted in Notional Ventures being selected as the security provider for the Cosmos Hub, a significant role that entails responsibility for the network's security infrastructure.

Details: - **Proposal Reference:** Proposal 104 - **Related Issue:** Interchain Security Issue #852

Concerns: - **Accountability:** Given the financial benefits received from ICF delegations, there may be perceived or actual conflicts of interest influencing the selection process and subsequent responsibilities.

P2P Storms

Overview: "P2P Storms" refer to a series of network exploits that have financially impacted various Cosmos-based projects, including Luna Classic and Osmosis. These incidents highlight vulnerabilities within the network's peer-to-peer communication protocols.

Details: - **Documentation:** Detailed reports are available in the p2p-storms folder. - **Chronology of Exploits:** - **Game of Zones (2020):** Identified by participants but not investigated. - **Sentinel (2021):** Sentinel Report - **Luna Classic (May 2022):** Potential oracle manipulation exploiting CosmWasm and CometBFT vulnerabilities. - **Stride (August 2023):** Network experienced 80-second long blocks due to transaction spam and missing IBC antehandlers. - **Osmosis (December 2023):** Financially consequential exploits demonstrating the deniability of blockchain attacks.

Concerns: - **Inadequate Response:** The ICF's lack of investigation into these vulnerabilities may have exacerbated financial losses and undermined network security. - **Preventative Measures:** Early detection and remediation of P2P Storms could have mitigated the impact of subsequent exploits, such as Luna's UST stablecoin failure.

Banana King: Lack of Field Length Limitations in IBC

Overview: The "Banana King" issue pertains to the absence of field length limitations within the Inter-Blockchain Communication (IBC) protocol, creating potential avenues for network attacks.

Details: - **Initial Reports:** - Reported by [@ctrl_felix](https://x.com/@ctrl_felix) via ICF's formal security reporting process. - Subsequently reported by [@getcoldy](https://x.com/@getcoldy) and directly to me. - **Public Documentation:** Lack of Field Length Limitations in IBC - **Analyst Confirmation:** Verified by a Web3 Analyst in Web3 Analyst's Report. - **Impact Example:** Example Banana King Transaction

Concerns: - **Security Risks:** The vulnerability allows for timing-based attacks, which can be exploited to disrupt network operations. - **Neglected Patches:** Despite multiple reports and an initial patch submission in 2022, the issue remains unresolved, leaving Cosmos chains susceptible to potential attacks.

IBC Version 3.0.0 and the Cosmos Hub

Overview: The Cosmos Hub's utilization of an obsolete version of the Inter-Blockchain Communication (IBC) protocol, specifically version 3.0.0, has led to security vulnerabilities and financial consequences for users.

Details: - **Vulnerabilities in IBC v3.0.0:** - **Dragonberry Vulnerability:** Exposes the network to potential exploits. - **ICA Channel Creation:** Requires the use of the counterparty's module name, allowing attackers to block ICA channel creation. - **Exploitation Incident:** Two weeks after reporting the use of IBC v3.0.0, the Cosmos Hub experienced an exploit resulting in 30,000 ATOMs of user funds being inaccessible. - **Reporting Timeline:** - Initial reports submitted to both the ICF and Informal Systems regarding the use of deprecated IBC versions.

Concerns: - **Delayed Remediation:** The continued use of deprecated protocols despite known vulnerabilities compromises the network's security and user trust. - **Financial Impact:** Users faced significant financial losses due to inaccessible funds, highlighting the severity of the oversight.

Financial Implications

The financial ramifications of the identified security vulnerabilities and exploit incidents are substantial:

- **Delegations and Revenue:**
  - Notional Ventures received over 800,000 ATOMs in delegations from the ICF, generating approximately $60,000 annually.
- **Economic Losses:**
  - A reported issue led to over $70 billion in economic losses due to an inaccurate report published by the ICF.
- **Exploit Consequences:**
  - The exploit of the Cosmos Hub resulted in 30,000 ATOMs being locked, directly impacting user funds and trust in the network.

These financial impacts underscore the critical need for transparent reporting, timely remediation of vulnerabilities, and accountable governance within the Cosmos ecosystem.

Retaliation and Safety Concerns

Personal Experience: Engaging in direct and public reporting of security issues within the Cosmos ecosystem has led to personal and professional retaliation. This includes:

- **Harassment:** Facing hostile responses from the ICF when raising legitimate security concerns.
- **Economic Threats:** Incurring costs to issue legal threats against the ICF to address inaccuracies in published reports.
- **Professional Repercussions:** Potential damage to career prospects and business operations due to public disputes with the ICF.

Concerns for the Community: - **Fear Among Colleagues:** Other ecosystem participants share fears of retaliation, which may discourage the reporting of security issues and hinder collaborative efforts to enhance network security. - **Safety of Individuals and Families:** The potential for personal retaliation poses significant risks to the well-being of those involved in reporting and addressing security vulnerabilities.

Recommendations

To address the identified issues and enhance the security, transparency, and trustworthiness of the Cosmos ecosystem, the following recommendations are proposed:

1. **Enhance Transparency:**
   - **Action:** Publish comprehensive delegation records and financial transactions involving the ICF and associated entities.
   - **Benefit:** Mitigates potential conflicts of interest and builds trust within the community.
2. **Standardize Security Reporting:**
   - **Action:** Align the security reporting policies across all contractors and platforms, ensuring consistency and clarity.
   - **Benefit:** Facilitates effective handling of security issues and prevents policy manipulation post-reporting.
3. **Strengthen Governance:**
   - **Action:** Establish independent oversight bodies to review security reports and policy changes within the Cosmos ecosystem.
   - **Benefit:** Ensures unbiased decision-making and accountability in addressing vulnerabilities.
4. **Implement Timely Remediation:**
   - **Action:** Prioritize the resolution of reported security vulnerabilities, especially those with significant financial implications.
   - **Benefit:** Reduces the risk of exploitation and protects user funds.
5. **Foster a Safe Reporting Environment:**
   - **Action:** Create channels that protect the anonymity and safety of individuals reporting security issues.
   - **Benefit:** Encourages the reporting of vulnerabilities without fear of retaliation.
6. **Provide Clear Documentation:**
   - **Action:** Develop comprehensive documentation and glossaries for technical terms used in reports.
   - **Benefit:** Enhances accessibility and understanding for non-technical stakeholders and bureaucrats.
7. **Promote Objective Communication:**
   - **Action:** Adopt a neutral tone in all communications, avoiding subjective language and ensuring balanced perspectives.
   - **Benefit:** Enhances professionalism and credibility of reports.
8. **Conduct Regular Audits:**
   - **Action:** Perform periodic security and financial audits of the Cosmos Hub and associated entities.
   - **Benefit:** Identifies and addresses vulnerabilities proactively, maintaining network integrity.

Conclusion

The Cosmos ecosystem plays a significant role in the decentralized blockchain landscape, with the Interchain Foundation at its core. However, the identified security vulnerabilities, inconsistent reporting policies, and instances of retaliation pose serious threats to the network's stability and user trust. Addressing these issues through enhanced transparency, standardized security protocols, and supportive reporting mechanisms is imperative to safeguard the ecosystem's future and uphold its integrity.

Glossary

- **FASF:** Swiss Financial Supervisory Authority.
- **ICF:** Interchain Foundation, an organization responsible for supporting the development of the Cosmos ecosystem.
- **IBC:** Inter-Blockchain Communication protocol, facilitating interoperability between different blockchains within the Cosmos network.
- **P2P Storms:** Network exploits targeting peer-to-peer communication protocols, leading to financial and operational disruptions.
- **Amulet:** Security contractor for the Interchain Foundation.
- **HackerOne:** A platform for reporting and managing security vulnerabilities.
- **ATOM:** The native cryptocurrency of the Cosmos Hub.
- **CometBFT:** A consensus engine used by the Cosmos network.
- **ICA Channels:** Interchain Accounts Channels, part of the IBC protocol facilitating account interactions across blockchains.

- **Dragonberry Vulnerability:** A specific security vulnerability associated with IBC version 3.0.0.

Appendices

Appendix A: Detailed Incident Reports

- **Fee Market Bug Report**
- **Sentinel Report**
- **Luna Classic Exploit Analysis**
- **Osmosis Exploit Analysis**
- **Web3 Analyst's Confirmation**
- **Interview with Jessica**

Appendix B: Supporting Documentation Links

- **ICF Delegation Information**
- **Proposal 104 Details**
- **Interchain Security Issue #852**
- **Juno Network Announcement**
- **Banana King Issue**