amulet

Transparency report

The Interchain Stack Security Program

august 1, 2023 -
september 30, 2024

Prepared by

Jessy Irwin,
CEO and Principal Security Engineer, Amulet

Moshe Mizrahi,
Principal Security Engineer, Amulet

Shawn Ellis-Sofer
Project Coordination Lead, Amulet

Introduction

In July 2023, Amulet kicked off a long-term security engagement with the Interchain Foundation (ICF) to build a robust and comprehensive security program for the Interchain Stack. The goal of the engagement was to ensure strong, scalable incident response capacity, create resilient security coordination and patching processes, and recalibrate the strategy and day-to-day operations of the Cosmos Bug Bounty Program as a public good.

As part of the first phase in a multi-year investment in security designed to yield immediate results in vulnerability disclosure, incident response, and security coordination, the Amulet team rapidly designed, built, and executed research-backed, state-of-the-art operational practices for the Interchain Stack and its stewards.

Transparency reports provide invaluable insights into an ecosystem's security posture, fostering trust and accountability in day-to-day security operations. This report is an artifact of the investments made by the Interchain Foundation and the distributed development teams that build and maintain its core protocols. By shedding light on security practices, including vulnerability disclosure, incident response, and security coordination processes, this report aims to improve the resilience of the broader Interchain ecosystem while promoting collaboration and continuous improvement.

The Interchain Stack Bug Bounty Program

The primary goal of a vulnerability rewards program is to incentivize the disclosure of security vulnerabilities. Ultimately, a bug bounty program is a harm reduction effort: By working closely with researchers who have discovered valid security vulnerabilities in production code, security teams can identify and fix vulnerabilities before attackers can exploit them.

When security teams launch a program and exchange information about vulnerabilities in code, they are purchasing information that, if wielded effectively, will improve the security maturity of a development team. By targeting specific classes of vulnerabilities and systematically addressing the root causes of each, it is possible to eliminate entire classes of vulnerabilities (and regressions) from a codebase.

Receiving bug reports is a normal part of day-to-day security operations. To support the decentralized nature of Interchain Stack development teams, Amulet has rapidly designed and implemented processes aligned with ISO/IEC 29147 29147:2018 (E) Information Technology—Security techniques—Vulnerability disclosure, the state-of-the-art international standard authored by the foremost experts in vulnerability disclosure worldwide. Aligning program processes and standards with this framework ensures that the Interchain Foundation and Amulet operate at the highest vulnerability coordination and disclosure standards.

Gap Assessment and Remediation

In the years leading up to 2023, the Cosmos Bug Bounty Program faced numerous challenges, including a significant backlog of more than 45 reports that had been open since 2020. Amulet performed a comprehensive gap assessment of Security resources and the existing bug bounty program, leading to numerous findings, including:

- Security reporting information in repositories across supported teams was either missing, incorrect, or non-standardized unsupported channels (e.g., Telegram and Discord), disincentivizing security reporters from focusing on the targets in-scope
- Security policies in repositories did not include safe-harbor reporting baselines to support safe and legal security research.
- Security policies in repositories did not set an expectation of bounty eligibility within the HackerOne program or official reporting channels.
- Program terms did not prevent core developers from “double-submitting” issues to the bounty program found during normal development.
- Over 45 unresolved issues were open in the program in various states of triage, with some reports being 3 years old.
- Supported versions eligible for bounties were not uniformly defined across all supported teams, leading to ambiguity of scope.

- Multiple issues in the program were handled poorly, resulting in unprofessional communications with reporters and requiring de-escalation communication.
- Lack of a standardized framework for categorizing and paying out bugs in a fair and repeatable fashion.
- Unnecessarily wide access to the bounty program results in issues being visible across teams, which increases the risk of information disclosure.
- Some in-scope properties for the program did not have a security contact or developer contact established, resulting in the mishandling of reports.
- Multiple issues that were explicitly out-of-scope for the program's focus on bugs in source code (IT Bugs, third party services, etc.) were paid out incorrectly to reporters.
- Lack of a grace period to allow for downstream consumers (e.g. chains) to adopt security fixes that were disclosed on an upstream asset (e.g. SDK) resulted in unnecessary double-payouts.
- Program participation significantly dropped off due to 2023 due to poor publicly-available performance metrics and payout scale.
- As of 7/26/2023, program response standards were at 53%, and had been as low as 27% during 2023, which negatively impacted the reputation of the program within the HackerOne platform and deters new researchers from participating.

Amulet identified and presented all of the above issues within the first month of the security engagement to the ICF, along with a comprehensive remediation plan to address the outstanding issues. All of the issues above were addressed and fully remediated within the first 30 days of ICF approval of the program rehabilitation plan.

As of 9/15/2023, Amulet addressed all outstanding reports in the program, which included de-escalation and retroactive amelioration of context with reporters in cases where communication was handled poorly, and retroactive bounty payments for some reports that were handled incorrectly.

As of 10/27/2023, Amulet deployed the new award structure, program policy, and scope, increasing program awards and clarifying scope for reporters.

After initial remediation, throughout Amulet's operation of the Bug Bounty, program response efficiency has remained at 100%.

Program Vision and Goals: 2023-2024

In September 2023, Amulet presented its pragmatic, tactical vision for a revamped bug bounty program that acts as a force multiplier for security in the Interchain ecosystem and:

- Provides an additional opportunity for security treatment in addition to automated testing and security vulnerability assessments.

- Consistently produces valid reports that identify bugs in software under development, preventing them from being shipped into production.
- Attracts a diverse set of hackers with varying skill sets and talents, which provide alternate perspectives about the code.
- Enables stewards and chain developers to rapidly patch and coordinate patching of critical and high severity issues before they are exploited in the wild, demonstrating a commitment to stewardship.
- Bolsters the reputation of the Interchain as the best technical solution for blockchain interoperability.

While the primary goal for 2023 was to restore the program to a healthy, performant state, in partnership with the ICF, we also sought to:

- Rapidly adopt researcher-first policy innovations, language, and perspective in the program policy that signals that Cosmos is a welcoming place for security research
- Champion adoption of best-in-class practices and coordination processes, and showcase their efficacy via consistent messaging and transparency reports
- Regularly assess what is working through blameless retrospectives, and to improve the experience for reporters working with the program.
- Address inefficiencies in the triage process (e.g. bug routing, missed targets) and set an appropriate, reasonable pace during the patching/advisory/security coordination process to help teams manage competing priorities.
- Expand program scope to be more inclusive of the Interchain Stack's most valuable components that have significant adoption, or that represent critical infrastructure.
- Shift the focus of the program on the Interchain Stack and core software components that have the highest impact on the security of the ecosystem.
- Implement bonus reward incentives (e.g. multipliers) as a tool to drive out specific classes of bugs from the Interchain Stack codebase.

Additionally, to attract top-tier bug reporters, it was critical to improve the onboarding experience so that anyone could quickly learn about the Interchain Stack and begin searching for bugs within minutes of discovering the program.

Program Scope

When Amulet took over the operation of the program, its scope had not evolved much since 2018, and it did not reflect the core software stack that powered the vibrant and growing Interchain Ecosystem.

To address this, over the past year, the scope of the Cosmos Bug Bounty Program has rapidly expanded to include several new components that are critical to the operation of the Interchain, including:

- Packet Forward Middleware
- CosmWasm
- Horcrux
- Hermes
- IBC-go Relayer
- 08-wasm light client

By adopting a comprehensive, component-based, agnostic view of ecosystem support and increasing code targets to include technology used by at least 33% of chains (or components with significant transaction throughput), the program better reflects the dynamic nature of the Interchain.

Program Policy

In September 2023, Amulet presented the Interchain Foundation with a new program policy that was designed to outline our "way of working" with security researchers, informed by firsthand experience of best practices and standards for security research. Since October 2023, the full policy for the Interchain Stack Bug Bounty Program has been available and up to date at hackerone.com/cosmos, and it includes:

- Program Rewards Tiers
- Coordinated Vulnerability Disclosure Policy
- Definitions for In-Scope and Out-of-Scope Issues
- Eligibility Rules for Bounty Rewards
- Confidentiality Expectations
- Official Channels Policy
- Good Faith Collaboration Policy
- Safe Harbor

To signal our commitment to collaborating with security researchers who may be new to blockchain protocols and the Interchain ecosystem, we chose to adopt the Coordinated Vulnerability Disclosure Policy and Safe Harbor Policy from disclose.io. This open-source policy is also included in the `security.md` files that outline vulnerability disclosure for components of the Interchain Stack.

In 2019, the Cosmos program was among the first in the blockchain space to adopt a Safe Harbor, a policy innovation that makes it clear that if legal action is initiated against a reporter by a third party, we will take steps to make it known that they complied with our program policy. By reintroducing this Safe Harbor with the support of the Interchain Foundation, the program has rejoined leading technology companies and visionaries at the forefront of researcher-first policy innovations.

To date, Amulet has not inhibited, prevented, blocked, or otherwise restricted any reporter from submitting issues to the HackerOne program or through the official Security Coordination channels.

Program Rewards

Bug Bounty Program Rewards from 2018 to 2024

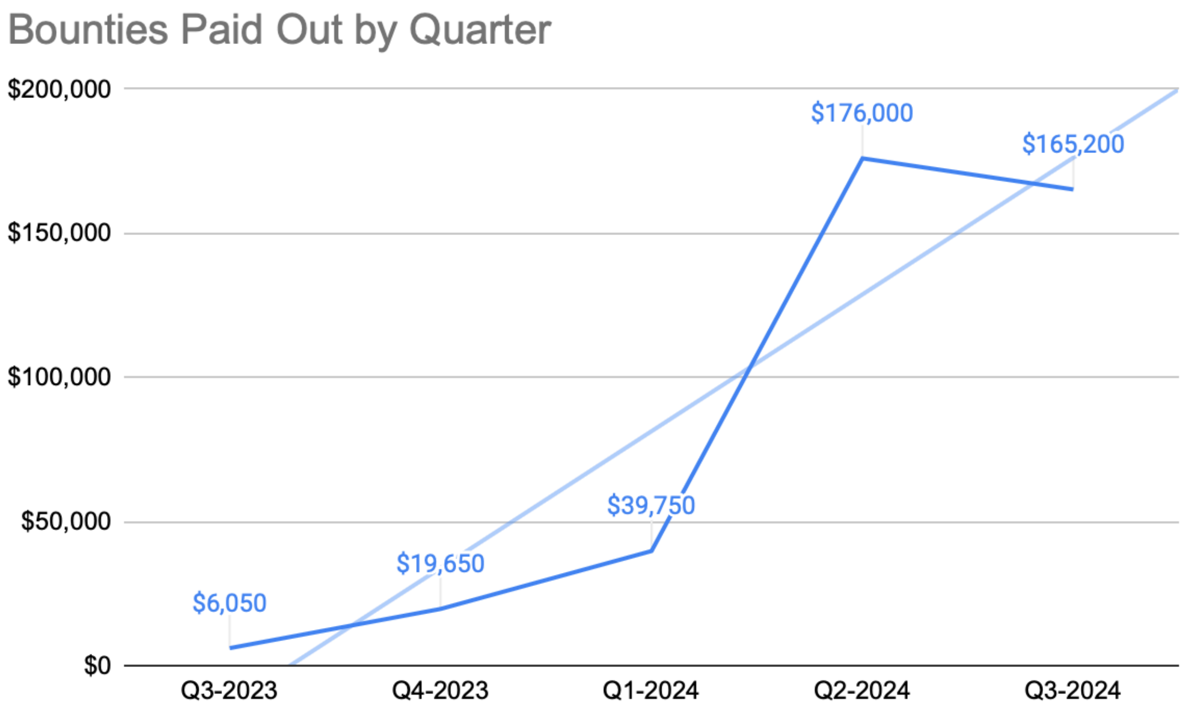
	May 2018	*October 2020*	*October 2023*	*October 2024*
Low	$100	$200	$1,000	$2,000
Medium	$500	$1,000	$3,000	$5,000
High	$1,000	$3,000	$10,000	$25,000
Critical	$2,500	$5,000	$25,000	$50,000

Program rewards for 2023-2024 start at the amount that is listed for each tier. The 90 day average for bounty rewards and percentage of total resolved reports is available for the program at hackerone.com/cosmos.

From May 2018 through July 2023, the Cosmos Bug Bounty Program paid out $133,050 in rewards to hackers who had reported bugs to the bug bounty program. From August 1, 2023 through September 30, 2024, under Amulet's administration, the program has paid out $407,400 in rewards for valid bugs.

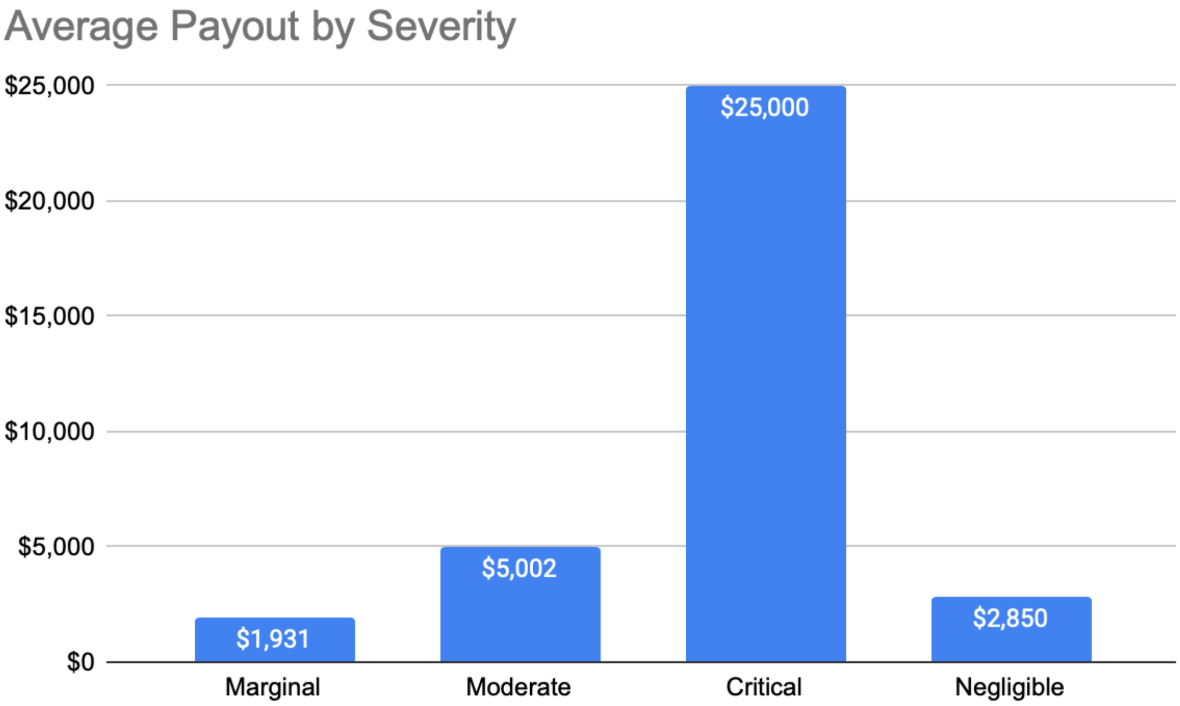
In October 2023, the program offered a 3x reward multiplier for valid CometBFT issues.

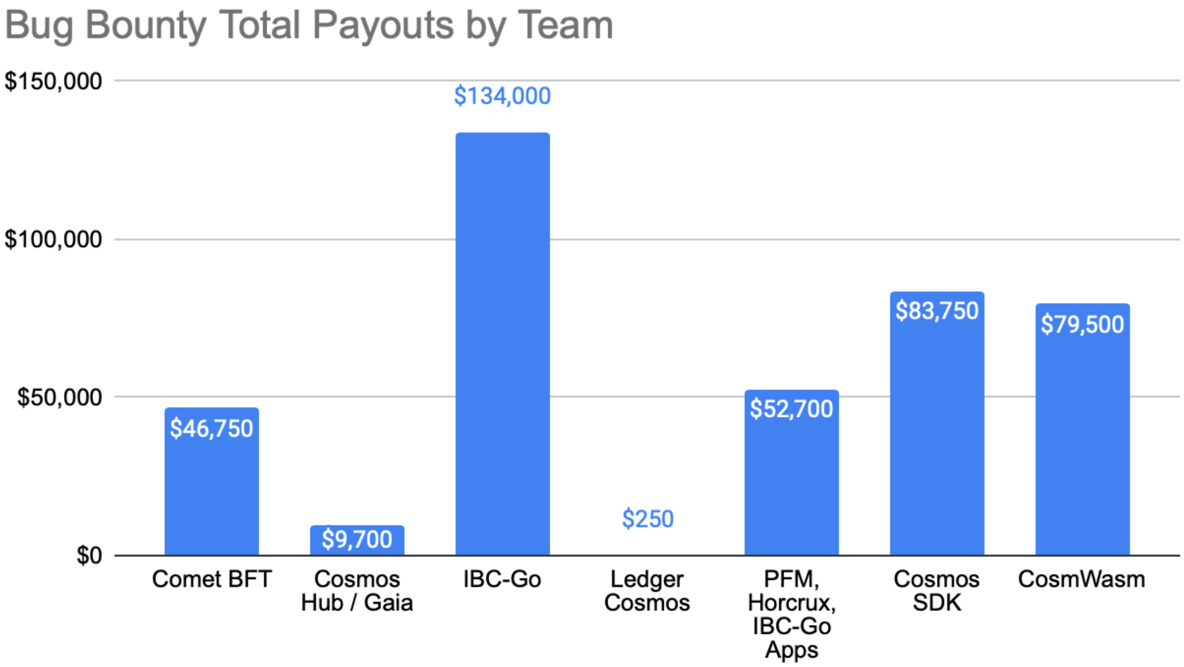
In May 2024, the program offered a 3x reward multiplier for valid IBC-go issues. In August 2024, this multiplier was extended through the end of the calendar year to December 31, 2024.



Prices for security vulnerabilities are determined by various factors, including issue severity, report quality, and reproducibility of the issue. As overpaying for security bugs undermines defenders without significantly reducing attacker stockpiles of vulnerabilities, it is critical for program health to ensure that rewards are carefully aligned towards the correct goals and incentives.

Program rewards are paid out to reports that represent valid, actionable security risk that report resulted in a code change, documentation change, security advisory, or reprioritization of an issue for a core team.


Average Payout by Severity
$25,000
$20,000
$15,000
$10,000
$5,000
$0
$1,931
$5,002
$25,000
$2,850
Marginal
Moderate
Critical
Negligible


Bug Bounty Total Payouts by Team
$150,000
$100,000
$50,000
$0
$46,750
$9,700
$134,000
$250
$52,700
$83,750
$79,500
Comet BFT
Cosmos Hub / Gaia
IBC-Go
Ledger Cosmos
PFM, Horcrux, IBC-Go Apps
Cosmos SDK
CosmWasm

As of September 30, 2024, the program has paid out $540,450 rewards total. The highest reward paid out for a valid bug bounty issue reported to the program is $100,000.

On October 1, 2024, Amulet increased the program rewards tiers for the program with the support of a robust program budget from the Interchain Foundation.

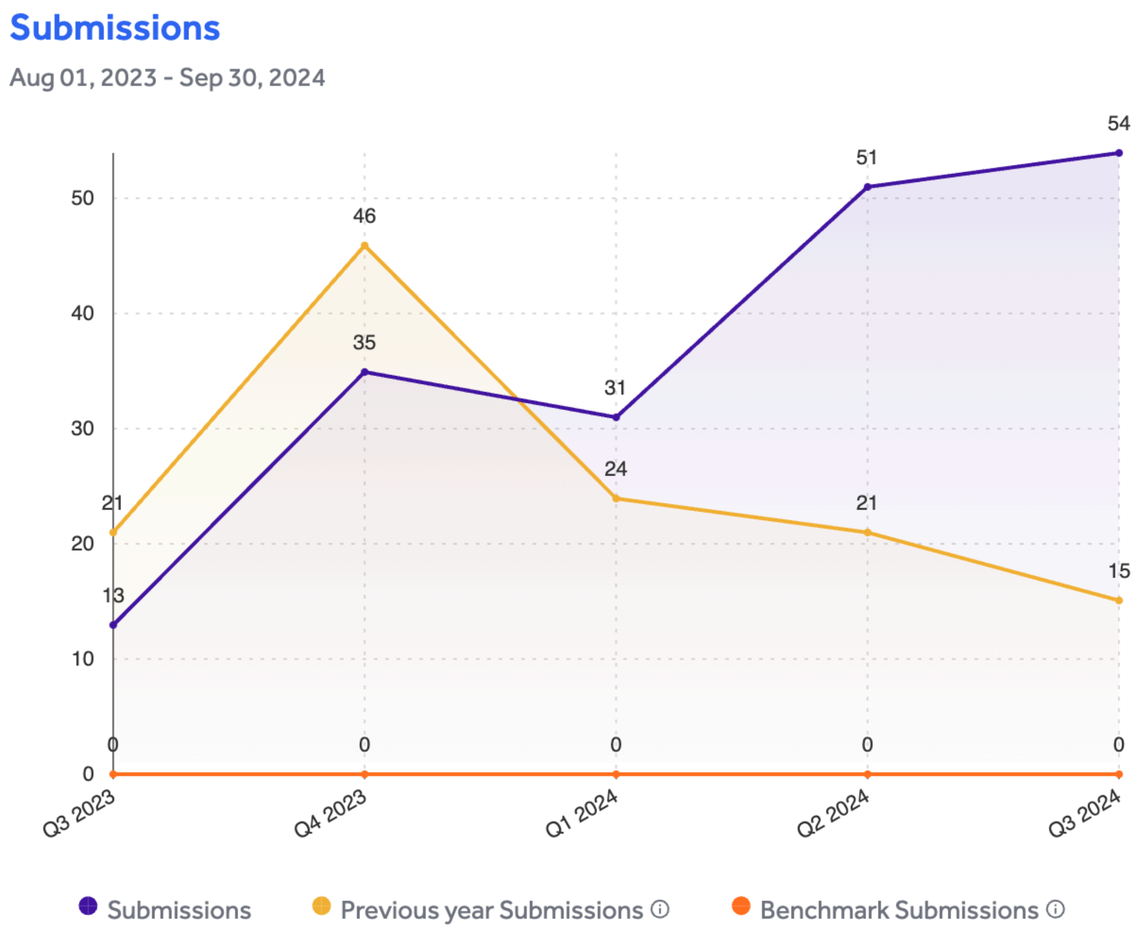
Program Milestones

August 2023	● Amulet gains access to HackerOne on August 7, 2023. ● Backlog of ~45 unresolved issues addressed for program participants; Inbox Zero achieved!
September 2023	● New program policy and strategy delivered to the ICF Board of Management for acceptance. ● Custom tooling is implemented to improve communication, route issues to Interchain Stack Teams, and gather performance metrics for teams participating in the program.
October 2023	● All program remediations, including new program policy, rewards, and strategy implemented after acceptance by the ICF Board of Management, ● Horcrux and Packet Forward Middleware are added to the program.
November 2023	● Shortly after implementing a new program policy, scope, and rewards tiers, Amulet sees a 10x increase in bug report submissions. ● Implemented a 3x reward for all valid CometBFT issues.
December 2023	● Long-time program participants begin to re-engage with the bounty program and submit new issues.
January 2024	● The CometBFT team resolved a high-severity issue in ~3 business days. ● Hermes and the IBC-go Relayer are added to the scope of the program. ● Achieved monthly high of $24,750 in rewards paid out to bug reporters.
February 2024	● Amulet learns new information about a vulnerability reported to the program, reassesses the severity to a higher level, and pays out additional rewards to the original reporter.

March 2024	● All available program performance metrics are publicly available on HackerOne for the first time in program history. ● Added the 08-wasm light client to the program.
April 2024	● The program awards the first six-figure bounty ever paid by the program for a valid Critical severity security vulnerability. ● The program exceeds all milestone targets for reaching a performant, healthy state less than six months after its strategy and operations refresh. ● A new Amulet BugTrack app launches to improve metrics tracking and communication with teams.
May 2024	● The Cosmos Bug Bounty Program turns six years old! 🎉 ● Implemented a 3x reward for all valid IBC-go bugs.
June 2024	● Recognized by HackerOne as a consistent, high-performing bug bounty program for Top Response Efficiency.
July 2024	● Continued to achieve a high signal-to-noise ratio of nearly 50% for bugs reported to the program. By contrast, many public bug bounty programs are considered successful if the signal-to-noise ratio is in the single digits.
August 2024	● Further clarified the inclusion of the Cosmos Hub in the existing program scope as a reference implementation for the Interchain Stack to better enable participants to identify bounty-eligible issues. ● Achieved the highest 90-day average for program reward payouts of $191,000. ● Updated the 3x reward payout multiplier for valid IBC-go issues to extend it through December 31, 2024.
September 2024	● Program recognized by HackerOne with the following decorations: ○ Top Response Efficiency, achieving and retaining response efficiency above 90% ○ Fast Payment, providing bounties within 1 month of receiving a vulnerability report ○ Gold Standard, adhering to the Gold Standard Safe Harbor reporting guidelines ● Program payouts reach all-time total of $540,450.
October 2024	● Rewards payouts are increased 100% with the support of a robust budget from the Interchain Foundation.

Program Performance Metrics

During the first two weeks of program administration, Amulet triaged all outstanding issues, demonstrating a commitment to operating the bounty program efficiently with an on-call rotation, and signaling to the public that the program rewards valid submissions promptly.



Data captured from HackerOne on 9/30/2024. Previous year Submissions shows program submissions over the same time period from the previous year, and Benchmark Submissions shows the median (50th percentile) of submissions for all HackerOne customers.

From August 1, 2023 through September 30, 2024, Amulet has:

- Evaluated **184 bug reports** in total, which is double the program submissions of the six months preceding this engagement.
    - Escalated 86 reports with actionable security impact to core teams.
    - Prevented 96 non-reproducible, invalid, or low-quality issues from distracting day-to-day development operations.
- Improved and maintained public-facing response metrics, re-igniting expanded external security researcher interest in the Interchain Stack.
    - Improved response compliance from 27% → **100%**.
    - Increased rewards by 100%, with Critical bugs now starting at $50,000.
    - Decreased average Time to Triage by 84% from 61 hours → **4 hours**.
        - Median Time-to-Response is 1 hour.
    - Decreased average Time to Close by 77% from 69 days → **20 days**.
        - Median Time-to-Resolution is 17 days.
- Awarded over $407,400 in bounty program payouts during our Administration of the program.
    - Average Time-to-Bounty: 16 days
    - Median Time-to-Bounty: 13 days.
- Engaged with more than **110 hackers** who submitted reports to the program.
- Coordinated discussion and remediation of issues across 15 scoped targets, spanning 9 decentralized development teams.
- Attracted many new high-quality reporters to the program while maintaining and growing relationships with existing high-signal, repeat contributors.
- Captured and successfully resolved the first Critical IBC vulnerability ever reported to the bounty program in 11 calendar days *without incident* during private security coordination.

Amulet also implemented custom automation and tooling, developed program metrics and documentation, and established relationships with product stewards to improve day-to-day security operations for the Interchain Stack. These efforts significantly reduced the time it took to resolve valid bugs, enhanced program transparency, and attracted more than 100 talented researchers to the program.

Program Performance by Component

Without the collaboration of the core teams, the Bug Bounty program would not be able to maintain high response efficiency, reporter retention, or a regular cadence of reports. The following section highlights metrics by core component, focusing on speed to response and severity of issue.

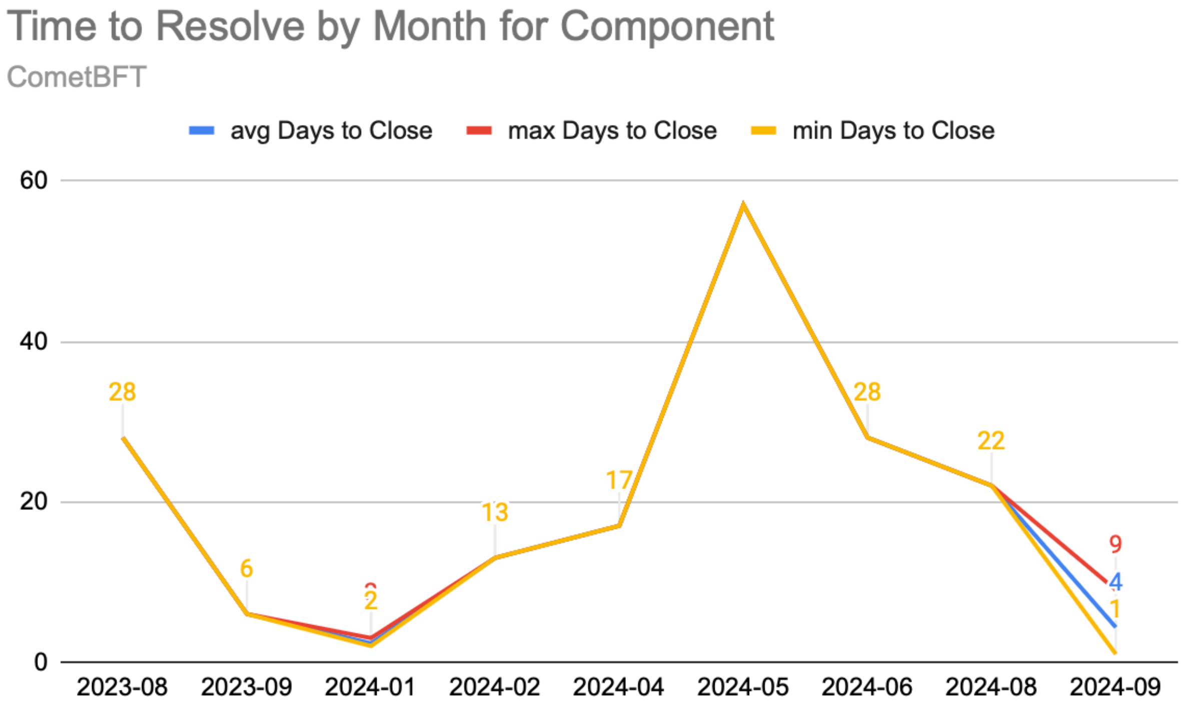
Between August 1, 2023 to September 30, 2024, four components in the program received no bug reports: Hermes, TMKMS, signatory, and yubihsm.rs.

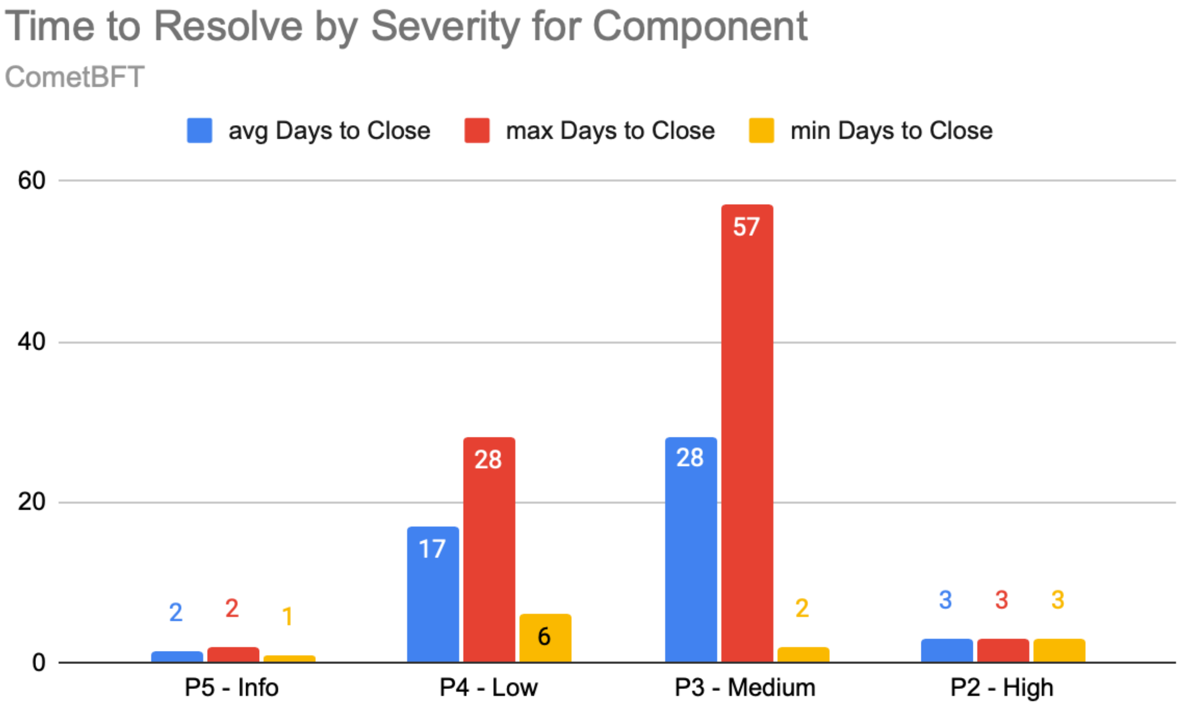
Component: CometBFT

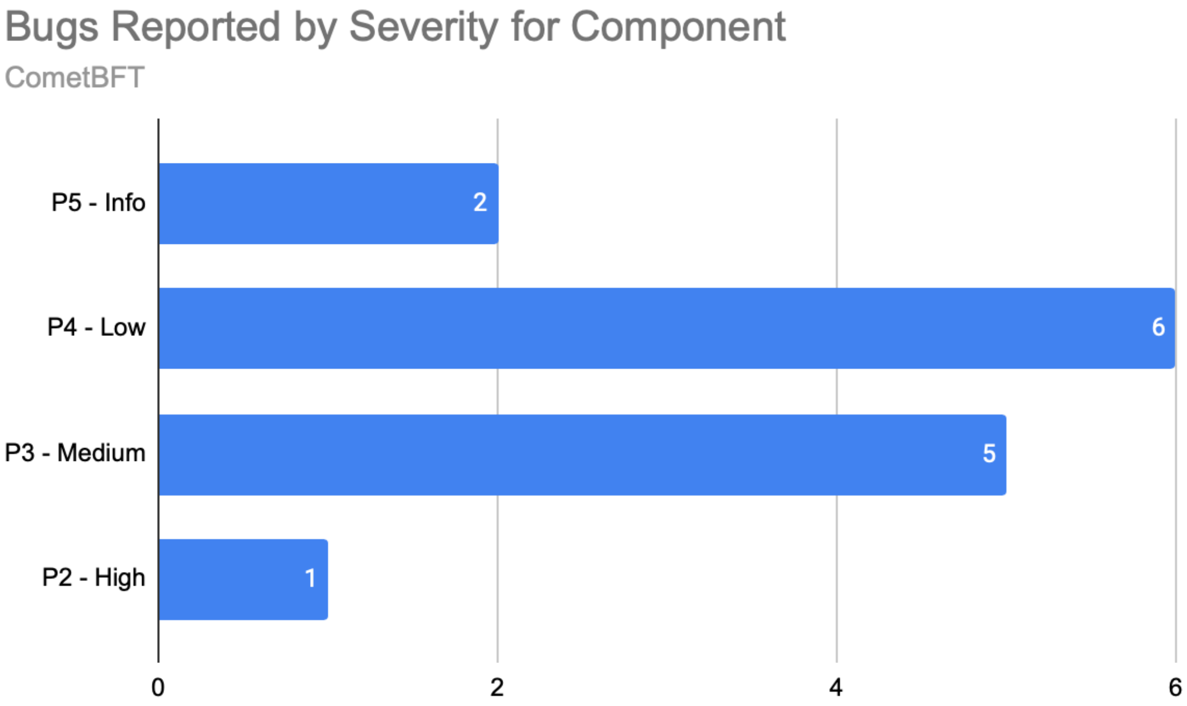
CometBFT is a blockchain application platform: it provides the equivalent of a web-server, database, and supporting libraries for blockchain applications written in any programming language. CometBFT implements Byzantine Fault Tolerant (BFT) State Machine Replication (SMR) for arbitrary deterministic, finite state machines.

For more background, see the CometBFT docs site. To get started quickly with an example application, see the quick start guide.

Development Team	**CometBFT, Informal Systems**
Total Reports Triaged for Component	**15**
Total Bounties Awarded for Component	**$46,750**




Time to Resolve by Severity for Component
CometBFT
avg Days to Close
max Days to Close
min Days to Close
60
40
20
0
P5 - Info
2
2
1
P4 - Low
17
28
6
P3 - Medium
28
57
2
P2 - High
3
3
3

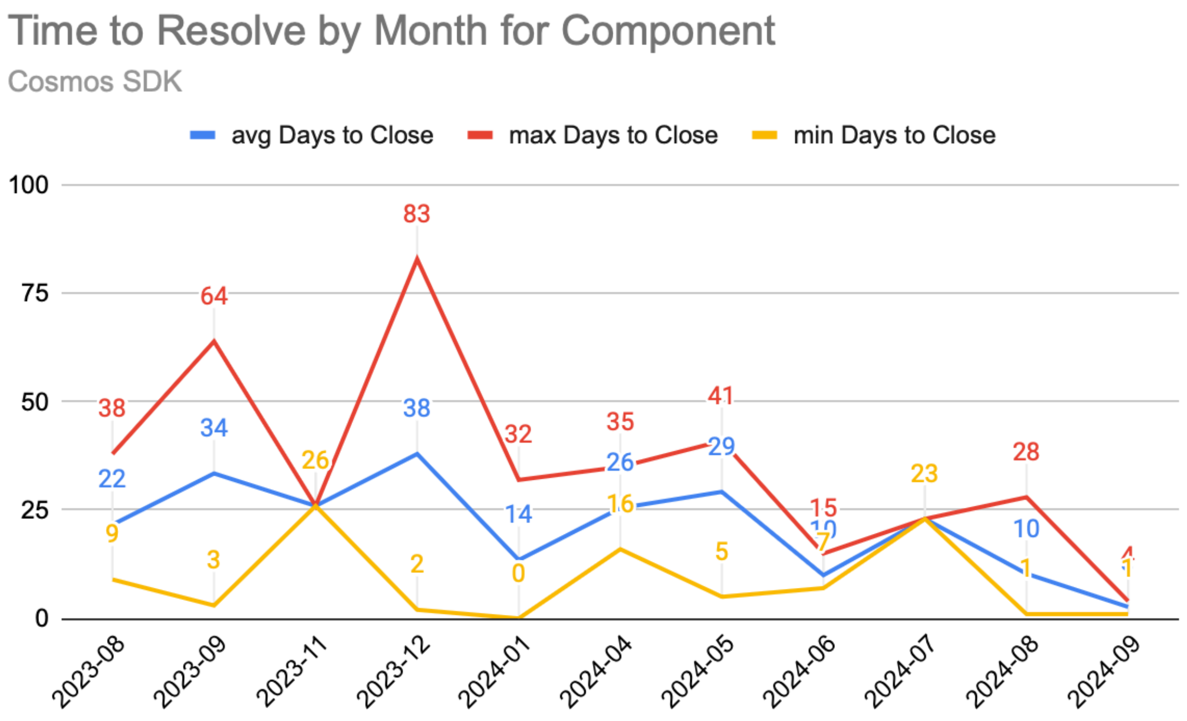

Bugs Reported by Severity for Component
CometBFT
P5 - Info
2
P4 - Low
6
P3 - Medium
5
P2 - High
1
0
2
4
6

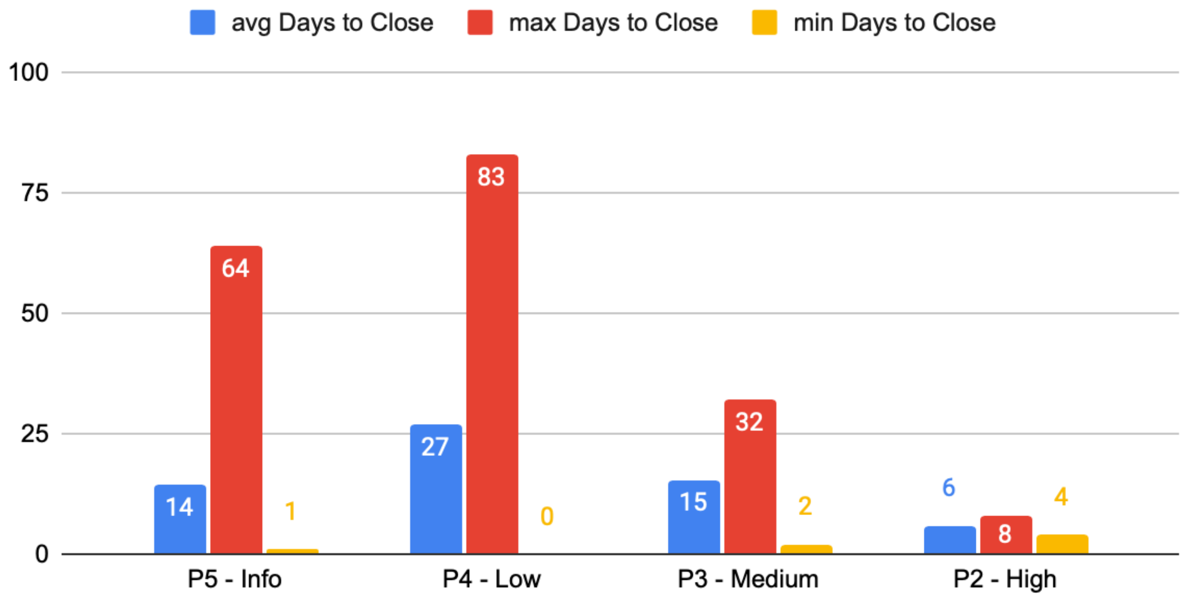
Component: Cosmos SDK

The Cosmos SDK is an open-source framework for building multi-asset public Proof-of-Stake (PoS) blockchains, like the Cosmos Hub, as well as permissioned Proof-of-Authority (PoA) blockchains. SDK-based blockchains are built out of composable modules, most of which are open-source and readily available for any developers to use.

To get started, learn more about the architecture of a Cosmos SDK application, or how to build application-specific blockchain from scratch with the Cosmos SDK Tutorial.

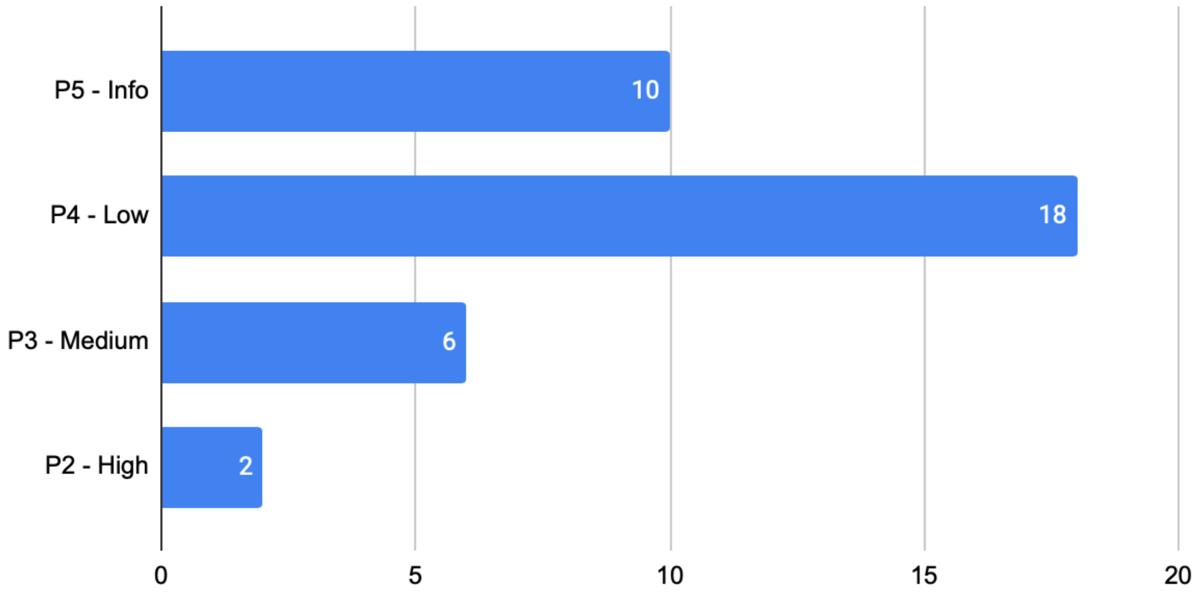
Development Team	**Binary Builders**
Total Reports Triaged for Component	**38**
Total Bounties Awarded for Component	**$83,750**





Time to Resolve by Severity for Component

Cosmos SDK



Bugs Reported by Severity for Component

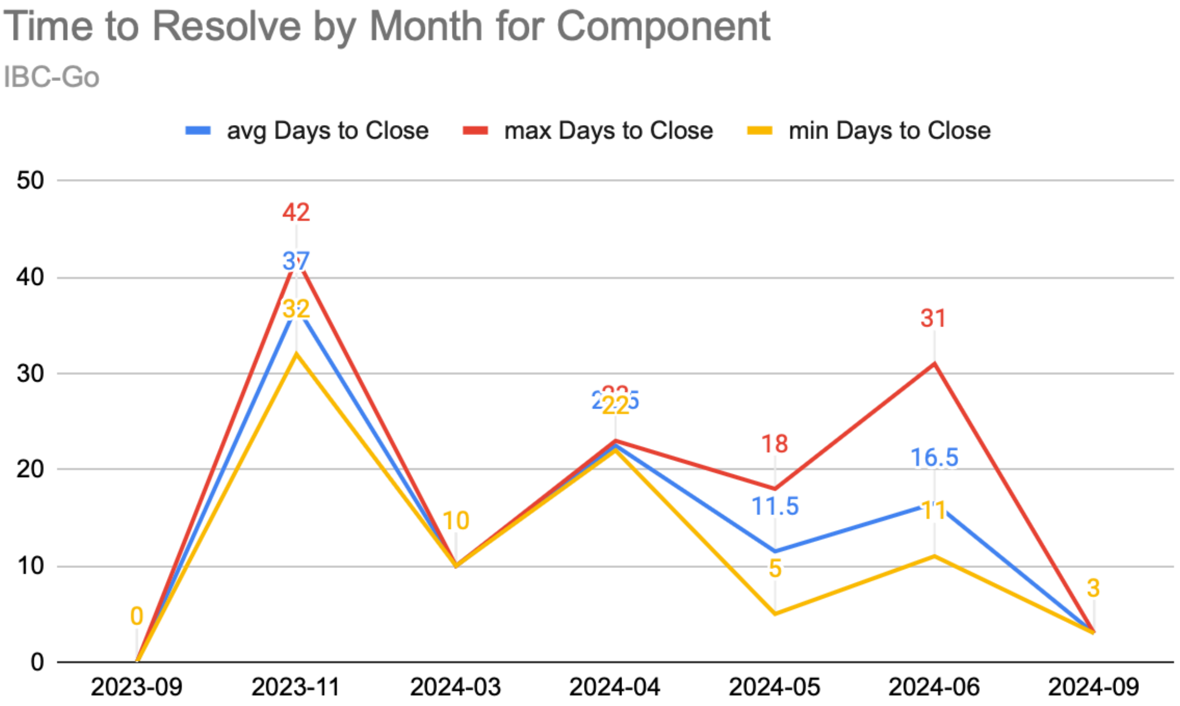
Cosmos SDK

Component: IBC-go

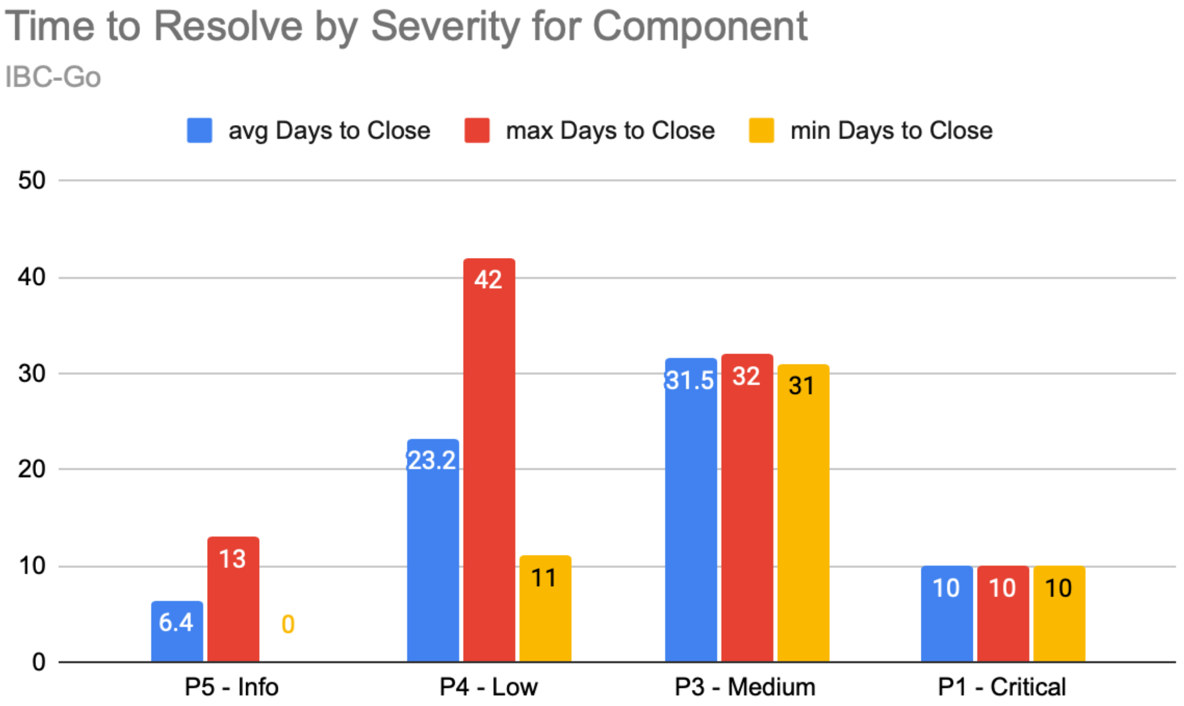
The Inter-Blockchain Communication Protocol (IBC) allows blockchains to talk to each other. The protocol realizes this interoperability by specifying a set of data structures, abstractions, and semantics that can be implemented by any distributed ledger that satisfies a small set of requirements.

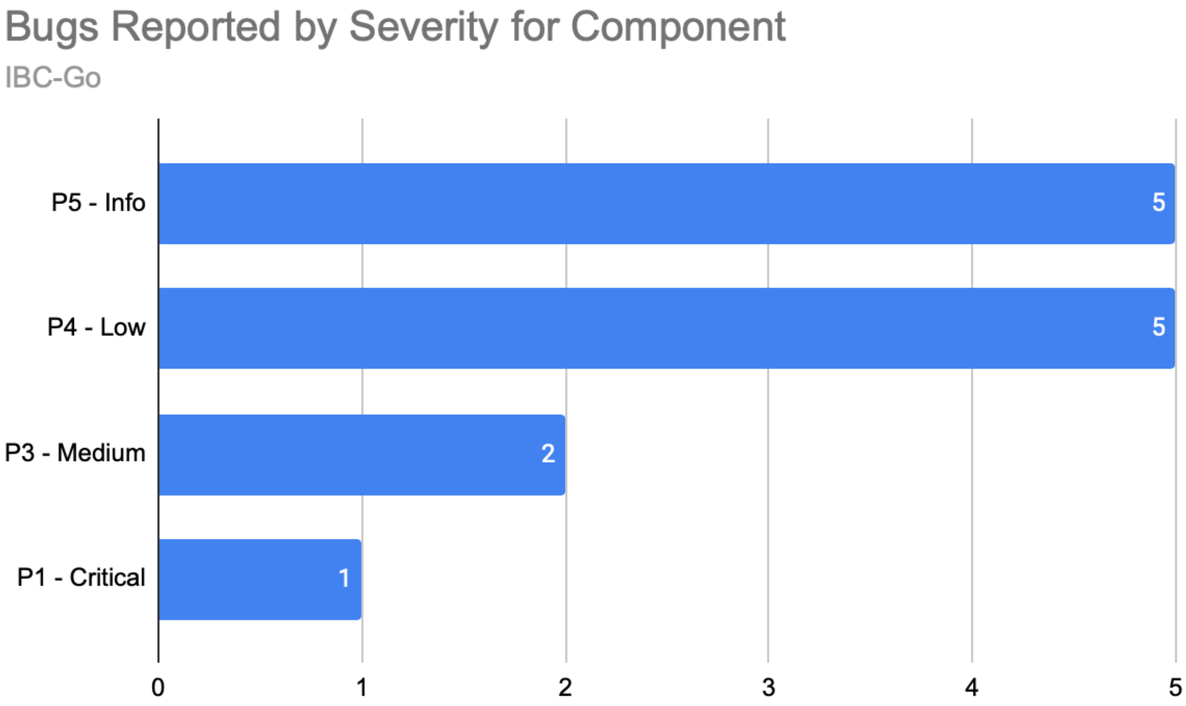
To learn more about IBC and its components, visit the documentation site.

Development Team	**Interchain GmBH**
Total Reports Triaged for Component	**13**
Total Bounties Awarded for Component	**$134,000**


Time to Resolve by Month for Component

IBC-Go


Time to Resolve by Severity for Component
IBC-Go
avg Days to Close
max Days to Close
min Days to Close
50
40
30
20
10
0
6.4
13
0
23.2
42
11
31.5
32
31
10
10
10
P5 - Info
P4 - Low
P3 - Medium
P1 - Critical

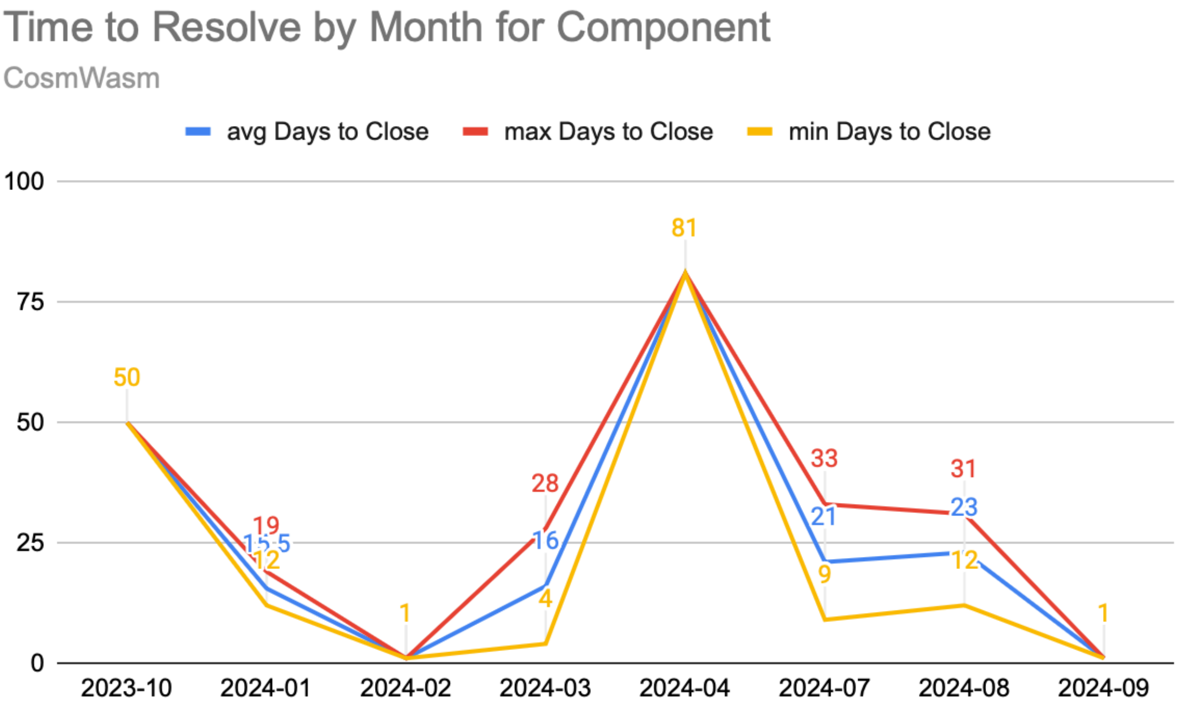

Bugs Reported by Severity for Component
IBC-Go
P5 - Info
5
P4 - Low
5
P3 - Medium
2
P1 - Critical
1
0
1
2
3
4
5

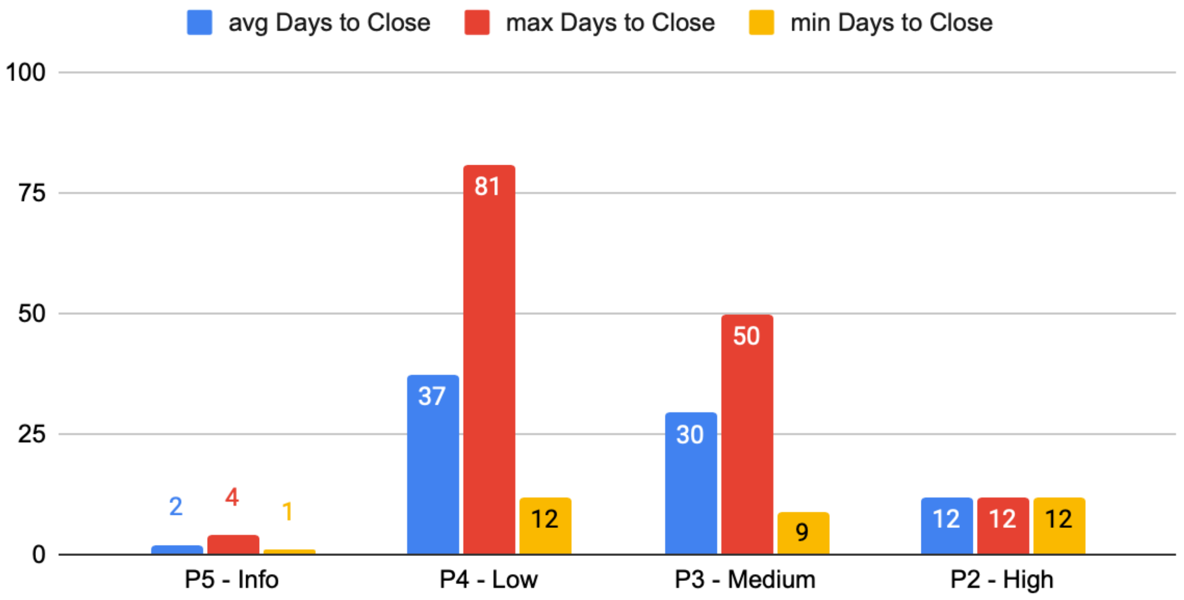
Component: CosmWasm

CosmWasm is a smart contract platform that focuses on security, performance and interoperability by Confio GMBH. It is the only smart contracting platform for public blockchains with significant adoption outside of the EVM.

For documentation about the platform and a Getting Started guide, please see https://www.cosmwasm.com/build.

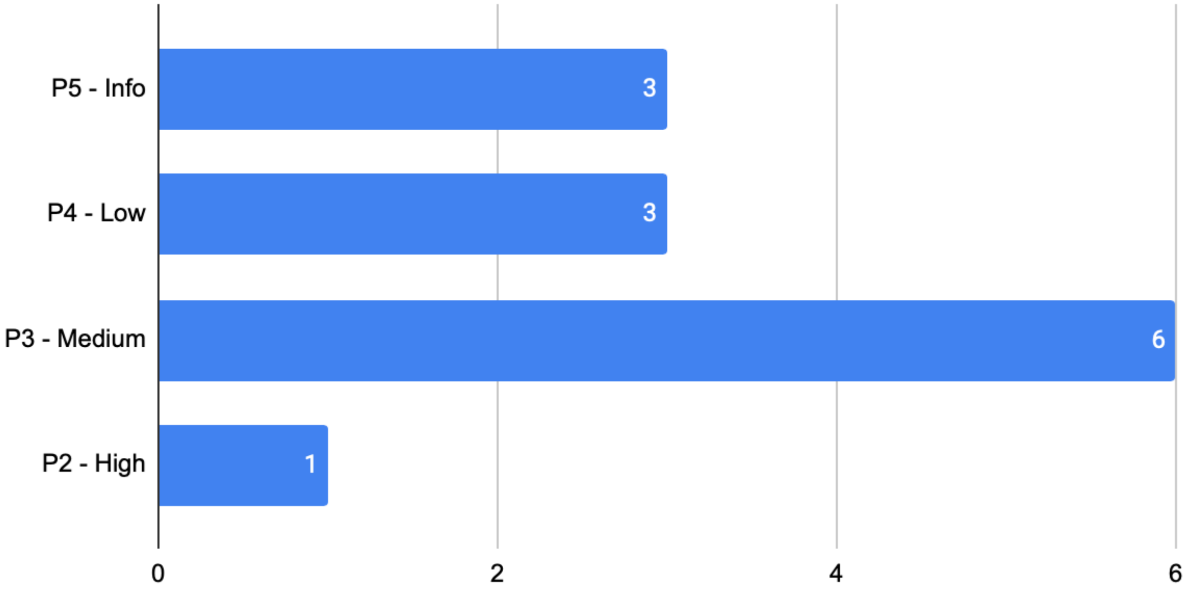
Development Team	**Confio**
Total Reports Triaged for Component	**14**
Total Bounties Awarded for Component	**$79,500**





Time to Resolve by Severity for Component

CosmWasm



Bugs Reported by Severity for Component

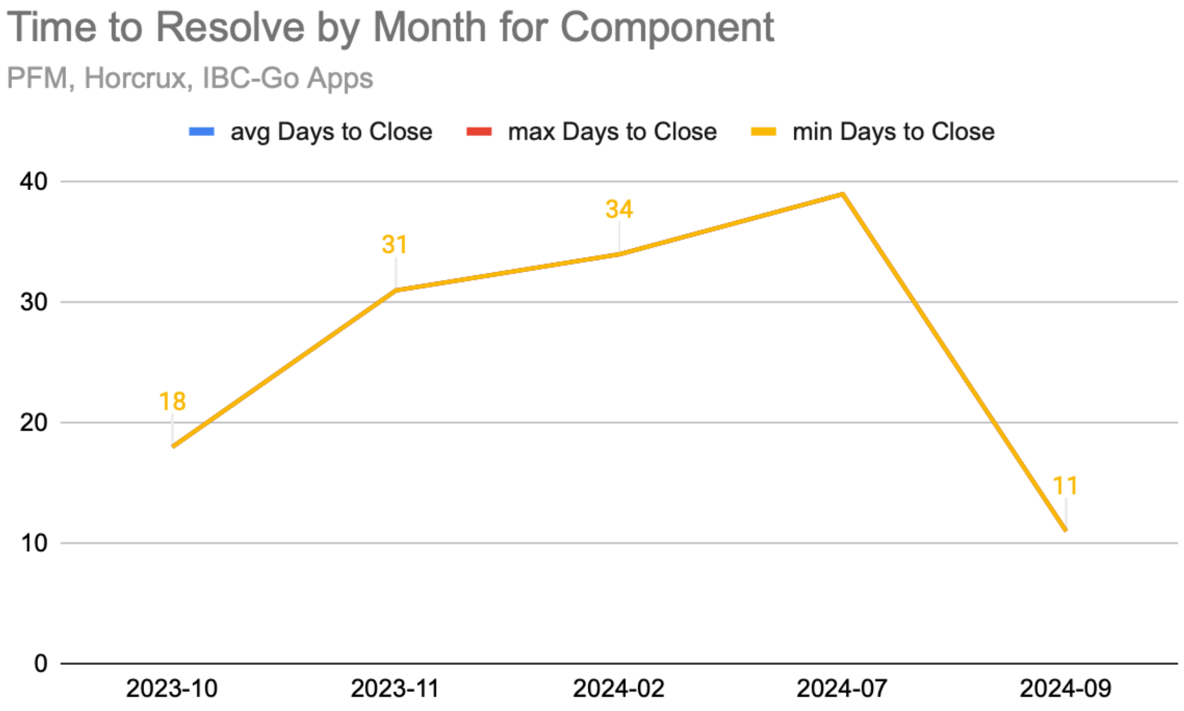
CosmWasm

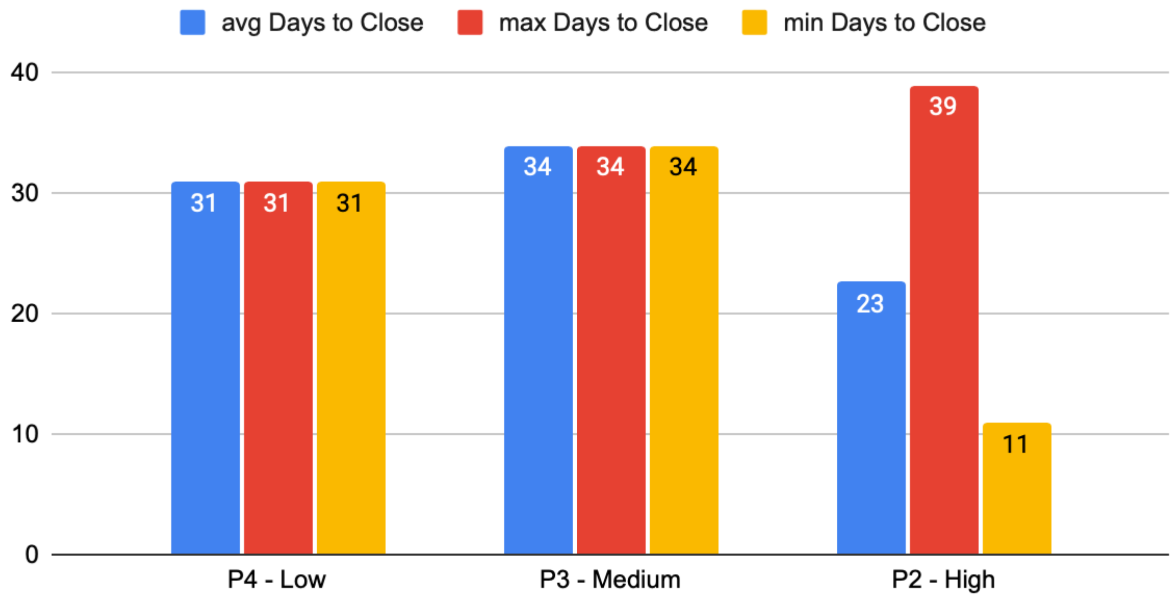
Component: Packet Forward Middleware, Relayer, Horcrux

The Strangelove team has 3 separate components within the scope of this program:

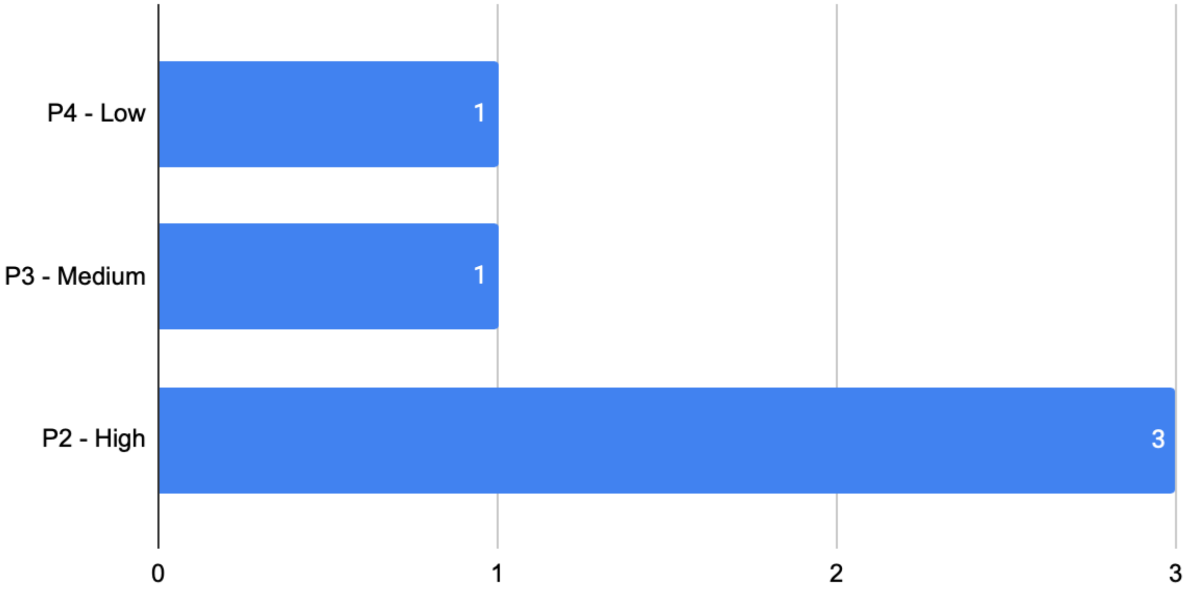
- **Packet Forward Middleware** (PFM) is an IBC middleware module built for Cosmos blockchains that routes incoming IBC packets from a source chain to a destination chain.
- The **IBC-go Relayer** is a Golang implementation of an Inter-Blockchain Communication Protocol (IBC) relayer maintained by Strangelove Labs. A relayer process monitors for updates on open paths between sets of IBC enabled chains and submits these updates in the form of specific message types to the counterparty chain.
- **Horcrux** is a multi-party-computation (MPC) signing service for CometBFT. It provides high-availability key management for Cosmos validator operations, and mitigates the risk of double signing transactions.

Development Team	**Strangelove**
Total Reports Triaged for Component	**5**
Total Bounties Awarded for Component	**$52,700**




Time to Resolve by Severity for Component

PFM, Horcrux, IBC-Go Apps

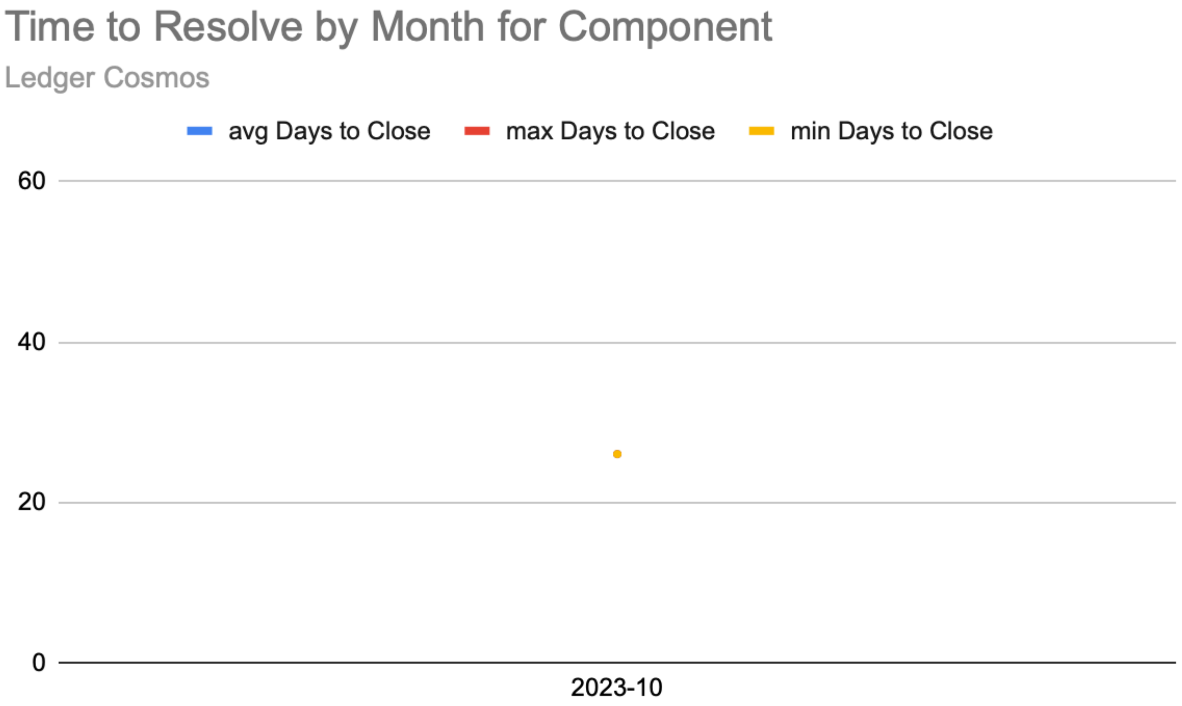

Bugs Reported by Severity for Component

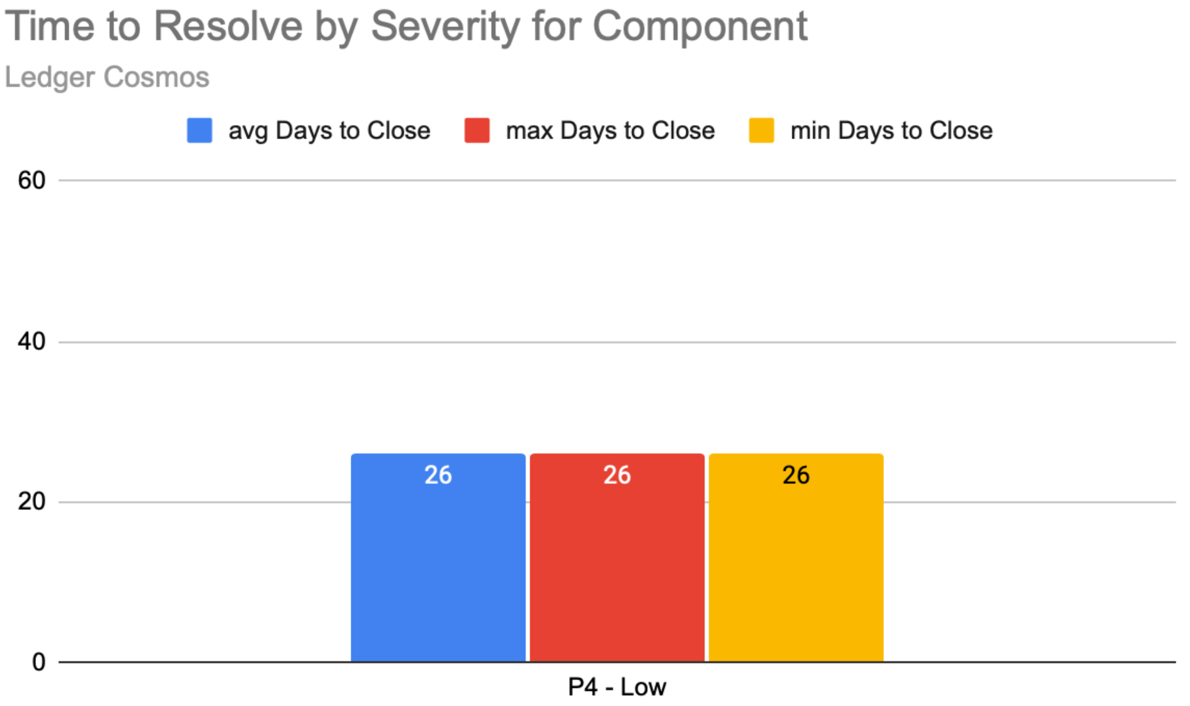
PFM, Horcrux, IBC-Go Apps

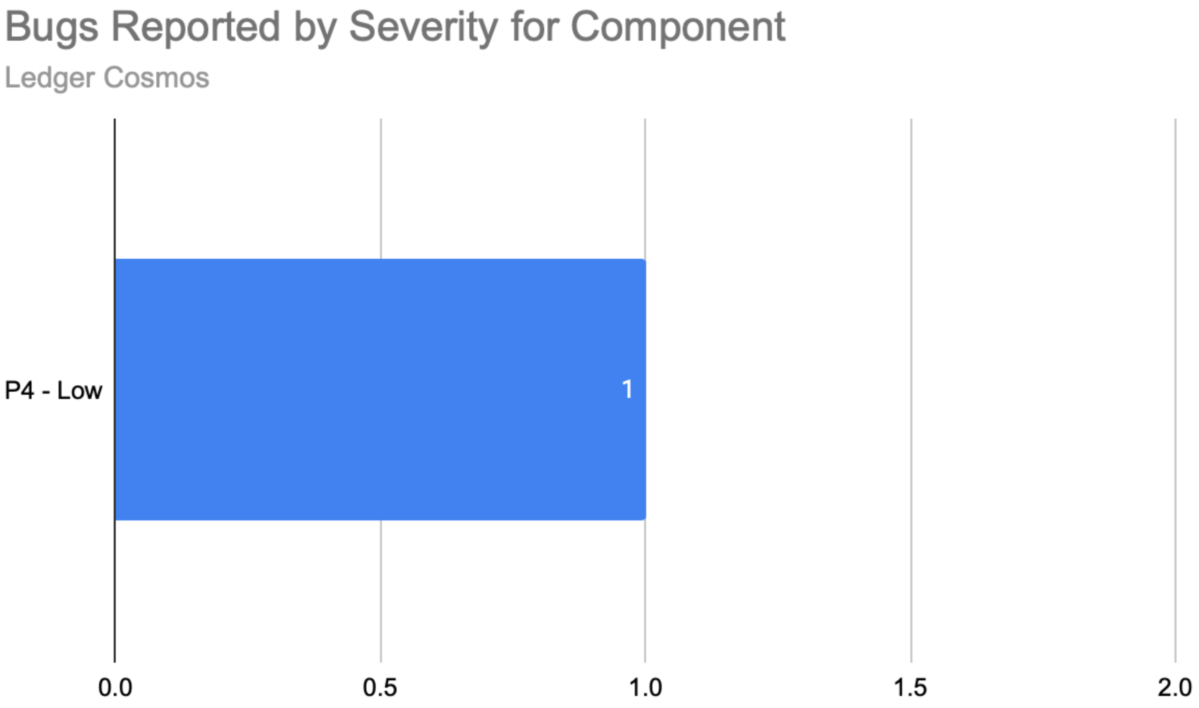
Component: Ledger-cosmos

Ledger-cosmos integrates Ledger's hardware wallet technology with the Cosmos ecosystem, providing a secure solution for managing Cosmos assets. By utilizing the Cosmos SDK, it allows for secure, cross-chain transactions while keeping private keys safely stored in Ledger devices. The integration aims to enhance security and usability in multi-chain environments, making it easier for developers and users to engage with the Interchain ecosystem.

Development Team	**Zondax**
Total Reports Triaged for Component	**1**
Total Bounties Awarded for Component	**$250**



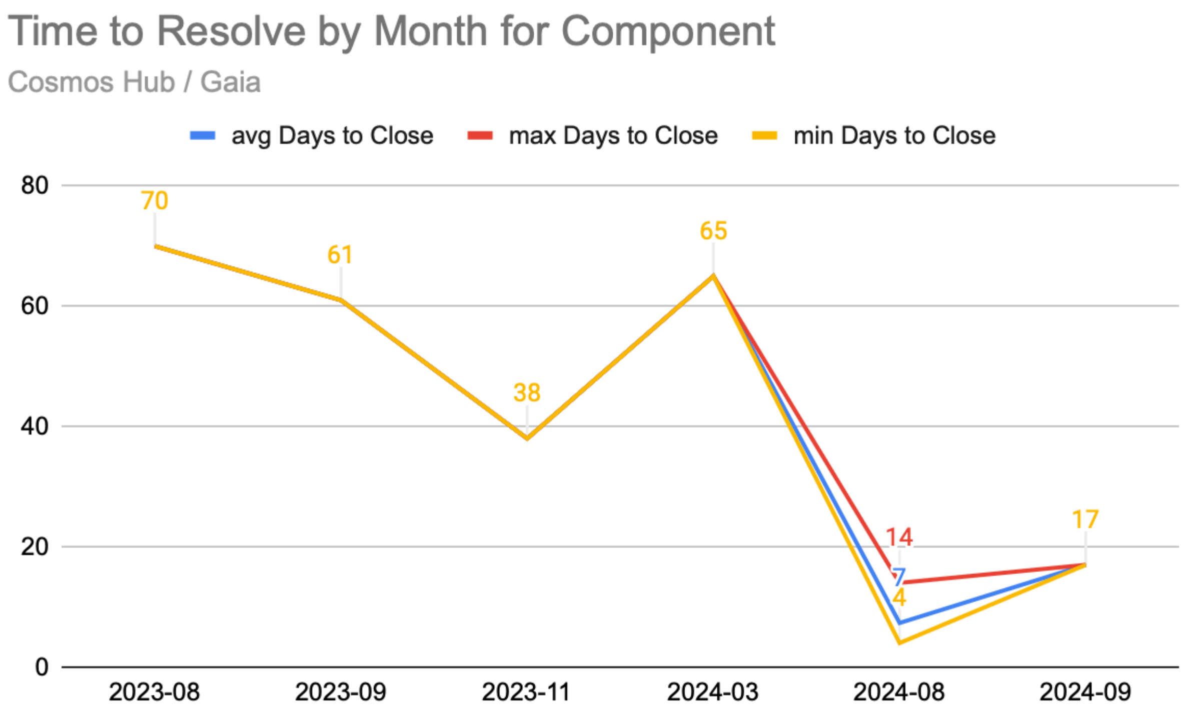

Time to Resolve by Severity for Component
Ledger Cosmos
avg Days to Close
max Days to Close
min Days to Close
60
40
20
0
26
26
26
P4 - Low

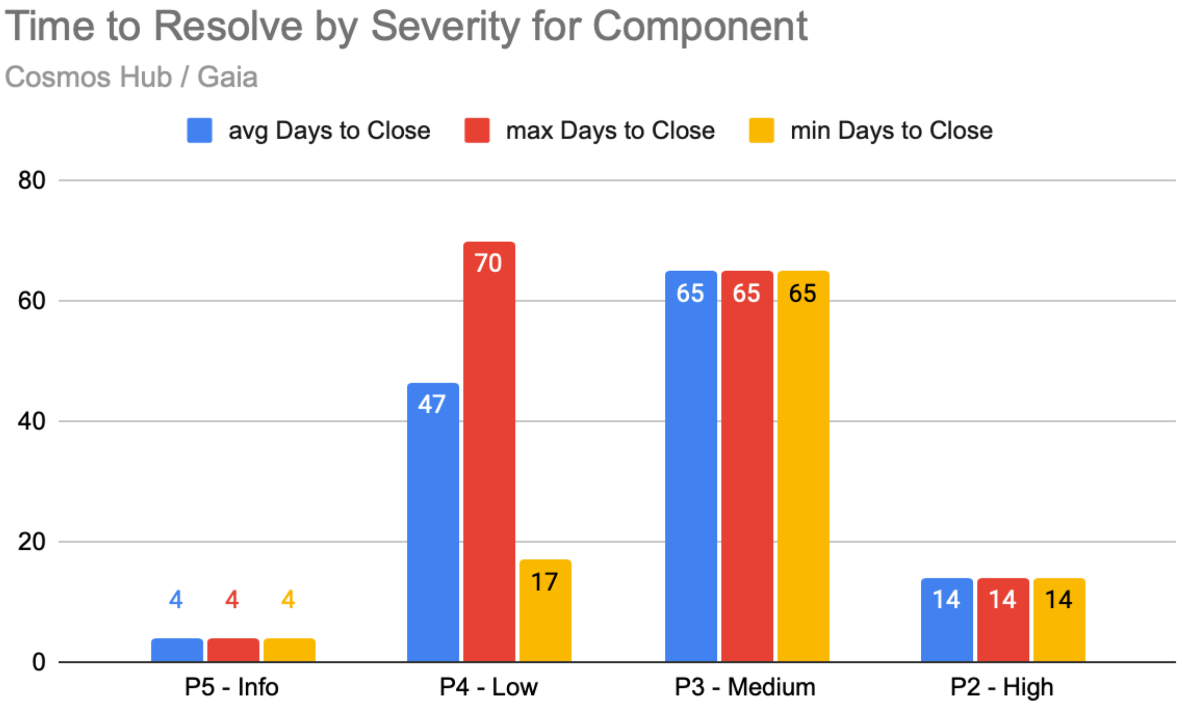

Bugs Reported by Severity for Component
Ledger Cosmos
P4 - Low
1
0.0
0.5
1.0
1.5
2.0

Component: Gaia (Reference Implementation)

Gaia is the app implementation for the Cosmos Hub, providing not only a base implementation of the Interchain stack, but also additional functionality from outside of the core Interchain Stack to support the needs of Cosmos Hub governance. Notable technologies that the Hub offers include an ICS implementation, liquid staking functionality, and extended fee market functionality.

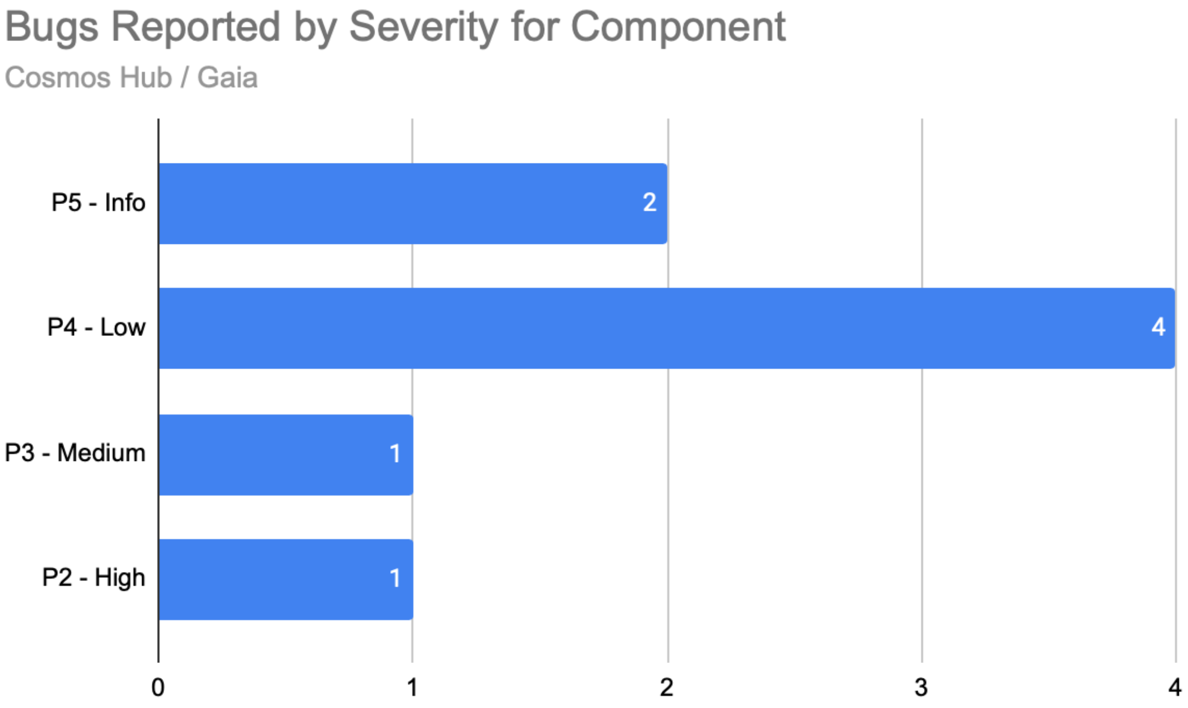
Development Team	**Cosmos Hub, Informal Systems**
Total Reports Triaged for Component	**8**
Total Bounties Awarded for Component	**$9,700**





Time to Resolve by Severity for Component

Cosmos Hub / Gaia



Bugs Reported by Severity for Component

Cosmos Hub / Gaia

Security Coordination for the Interchain Ecosystem

Multiparty coordinated vulnerability disclosure requires the collaboration of multiple stakeholders, including security researchers, platform developers, and ecosystem participants to ensure that vulnerabilities are disclosed and patched in a timely, efficient manner. This approach helps to mitigate the risks associated with vulnerabilities and protect chains, assets, and the people who depend on them. In the case of the Interchain ecosystem, however, many traditional governance models, security controls, and organizational models that come with security coordination are incompatible with decentralization and the operational complexities that come with it.

Responding to any security event in the Interchain ecosystem is challenging due to a variety of factors: shared protocol design risk, and worldwide multi-party coordination that can involve over hundreds (or thousands!) of individuals to act in the best interests of a chain and its community. In 2023, The Interchain Foundation invited Amulet to identify opportunities to improve and streamline security coordination to reduce risk and expedite faster security response.

Gap Assessment and Remediation

In August 2023, Amulet reviewed historical security artifacts and performed a gap assessment of existing security coordination capacity. During that assessment, we identified the following issues:

- There was no proactive, agreed-upon process in place to respond to security events.
- If security processes existed, most were not documented, repeatable, or scalable.
- There was a pattern of significant and repeated lapses of confidentiality and disclosure.
- There was no consideration for equity in regards to fairness and distribution of information; some chains felt that they had to be in the “in crowd” to get information about how a security issue would impact their use cases and ecosystems.
- Ineffective communication to chain developers, validators, and other ecosystem stakeholders.
- Outreach was ad-hoc, and relied on non-standardized contact information for chains, development teams, validators, and personalities spanning 12 different communication platforms.
- Lack of standardization of chain inventory sourcing for response efforts.
- Lack of infrastructure, tooling, and automation to support response efforts.

Throughout 2023-2024, Amulet worked closely with Interchain Stack development teams to transition towards a more robust, scalable security coordination process, and continued to mature program efforts, including:

- Clarifying roles and responsibilities around coordination across Interchain Stack development teams, ensuring seamless incident management, and driving the creation of security policies.
- Implementing structure and process across all Interchain Stack teams to simplify security coordination, patching, and response.
- Implementing a standardized security advisory system to distribute actionable information about security risks to code consumers leveraging Github's security advisory notification features.
- Providing extensive guidance to teams around incident lifecycle and communications to enable teams to best deliver security updates to their customers.
- Launching a signup for the security advisory list, fostering a community of security-conscious developers.
- Launching a content portal for Security-related topics, advisories, and open source methodology documentation for the Interchain community.
- Developing runbooks and security coordination plans for specific security scenarios.
- Developing custom tooling to support security coordination, enhancing response capabilities and identification of impacted parties.

Security Coordination Milestones

September 2023	● First ASA security advisories are released to provide actionable information about security risk to the Interchain ecosystem. ● Amulet adopts Github Advisories as the primary source of truth for security issues, and aligns ASA advisory format with this system.
October 2023	● Amulet and Strangelove successfully coordinate and resolve two High severity vulnerabilities in Packet Forward Middleware, Pigeonfall and Viperstrike.
November 2023	● Shortly after implementing a new program policy, scope, and rewards tiers, Amulet sees a 10x increase in bug report submissions. ● Long-time program participants begin to re-engage with the bounty program and submit new issues.
February 2024	● Amulet supports coordination for a High severity vulnerability in Packet Forward Middleware.

March 2024	● Amulet launches the /security repository to support private security coordination for High and Critical vulnerabilities. ● Amulet shares v.1 of the Interchain Stack Severity Classification Matrix.
April 2024	● The IBC-go team and Amulet coordinate to resolve a complex Critical severity issue submitted to the program in ~11 *calendar* days. ● Signed artifacts are used for the first time to support private security coordination for the Interchain Stack.
July 2024	● Amulet updates the Interchain Stack Severity Classification Matrix to better clarify the consequences of security issues for chain developers and validators.

Coordination Metrics

From August 1, 2023 through September 30, 2024, Amulet has:

- Released 11 security advisories for Interchain Stack components.
- Experienced 0 incidents of exploitation during security coordination, as confirmed by networks.
- Lead 1 security coordination event for a Critical vulnerability in IBC-go.
- Managed 9 additional security coordination events with Interchain Stack development teams.

As Amulet's engagement and program strategy are focused on the Interchain Stack, Amulet is not the directly responsible entity for any security response activities for the Cosmos Hub. All security response activities for the Cosmos Hub are the direct responsibility of its governance-mandated maintainers.

In addition to administering the Bug Bounty program for bounty rewards, Amulet also operates the security@interchain.io email as an Official Channel for coordinated vulnerability disclosure. Upon receiving a report that could benefit from upstream disclosure, regardless of scope, where it is possible, our team works with the corresponding chains, teams, and developers to coordinate a safe response that protects users.

To date, Amulet has responded to all incoming communications regarding coordinated vulnerability disclosure efforts and has not inhibited, prevented, blocked, or otherwise taken any actions to restrict anyone from utilizing our official channels to report security issues.

For more information about reporting issues for security coordination, please refer to https://github.com/interchainio/security.

Security Coordination Resources

/security

In 2024, Amulet launched `/security`, a repository for resources and information around Interchain Security topics at https://github.com/interchainio/security. In addition to security resources, this repository contains a listing of all issued Amulet Security Advisories (ASA) and signing identity information for Amulet.

Severity Classification Framework

To aid with vulnerability severity classification, the Amulet team developed a comprehensive risk classification framework, to help reporters and developers better quantify realized risk in the context of the Interchain Stack. Amulet utilizes this Impact and Likelihood model to classify and prioritize issues submitted to the Bug Bounty program as well as in security coordination and response. The risk matrix scale and terminology is calibrated for the unique needs of the Interchain Stack and overall community to best capture local chain vs. wide ecosystem impact.

Security Advisory Distribution List

Amulet created the Security Advisory Distribution List in 2024 as a means to collect contacts to notify for pre-release notifications and security advisory contents. This notification list is separated by component, so interested parties have the option to specify a specific Interchain Stack component to be notified about, or all and future components.

If you are interested in receiving security advisories about vulnerabilities discovered in the Interchain Stack, sign up for the security email distribution list here.

Emergency Security Coordination

If you are building on the Interchain Stack and want to ensure that your team is easy to contact in the event that you are impacted by a Critical security vulnerability, create a security contact email alias and include this information in a `security.md` in your main code repository. (Note: Before publishing your security contact, we highly recommend testing it to ensure that it can receive messages from outside of your email domain!) Maintaining a security contact is a best practice in the wider technology sector, and in the event that your chain implementation or source code is impacted by a security vulnerability in the Interchain Stack, we will contact you via email through this channel to coordinate patching and response. In addition to providing equitable access to information about security vulnerabilities to all recipients simultaneously, security contact email addresses (and distribution lists) have been an essential tool in the defender's toolbox for decades, especially for kicking off coordination of major multiparty vulnerability disclosure events like Heartbleed, Spectre, and Meltdown.

If you are a chain operator and you want to verify if Emergency Security Coordination for an Interchain Stack component is taking place, please reach out to our official channel by emailing security@interchain.io. Though the ICF, Amulet, and Interchain Stack teams cannot make public announcements about private security coordination activities, we can confirm if a communication you have received from a chain was prompted by ongoing security coordination and response efforts from our team.

Engaging with Security as a Public Good

If you believe you have found a vulnerability in the Interchain Stack or would like to contribute to the Cosmos Bug Bounty Program by reporting a bug, please visit https://hackerone.com/cosmos to submit a report.

If you are building on the Interchain Stack and want to ensure that your team is easy to contact if a Critical security vulnerability impacts your chain or source code, create a security contact email alias and include this information in a `security.md` file in your main code repository. Before publishing your security contact email address, test it and verify that it can receive messages from outside your organization's domain!

If you are a validator, you can improve security response coordination with chains by setting a security contact email address in your on-chain profile. Taking this step enables chain developers to quickly query the chain to gather contact information from network operators, and it may simplify and speed up communication during a security emergency.

If you are interested in receiving security advisories about vulnerabilities discovered in the Interchain Stack, sign up for the security email distribution list here.

If you are a member of an organization seeking to engage in B2B security vulnerability disclosure with Interchain Stack development teams, please contact security@interchain.io.

If you are a validator or chain developer and you want to verify if Emergency Security Coordination for an Interchain Stack component is taking place, please reach out to our official channel by emailing security@interchain.io. Though the ICF, Amulet, and Interchain Stack teams cannot make public announcements about private security coordination activities, we can confirm if a communication you have received from a chain was prompted by ongoing security coordination and response efforts.

Appendix

A – Raw Data: HackerOne Program Submissions by Quarter, August 1, 2023 - September 30, 2024

interval	Submissions	Previous year Submissions	Benchmark Submissions
Q3 2023	13	21	16
Q4 2023	35	46	20
Q1 2024	31	24	17
Q2 2024	51	21	19
Q3 2024	54	15	19

B – Raw Data: Time to Close by Severity By Team

Severity	Team	avg Days to Close	max Days to Close	min Days to Close
P5 - Info	Comet BFT	2	2	1
P5 - Info	CosmWasm	2	4	1
P5 - Info	Cosmos Hub / Gaia	4	4	4
P5 - Info	Cosmos SDK	14	64	1
P5 - Info	IBC-Go	6	13	0
P4 - Low	Comet BFT	17	28	6
P4 - Low	CosmWasm	37	81	12
P4 - Low	Cosmos Hub / Gaia	47	70	17
P4 - Low	Cosmos SDK	27	83	0
P4 - Low	IBC-Go	23	42	11
P4 - Low	Ledger Cosmos	26	26	26
P4 - Low	PFM, Horcrux, IBC-Go Apps	31	31	31
P3 - Medium	Comet BFT	28	57	2
P3 - Medium	CosmWasm	30	50	9
P3 - Medium	Cosmos Hub / Gaia	65	65	65
P3 - Medium	Cosmos SDK	15	32	2
P3 - Medium	IBC-Go	32	32	31
P3 - Medium	PFM, Horcrux, IBC-Go Apps	34	34	34
P2 - High	Comet BFT	3	3	3
P2 - High	CosmWasm	12	12	12
P2 - High	Cosmos Hub / Gaia	14	14	14
P2 - High	Cosmos SDK	6	8	4
P2 - High	PFM, Horcrux, IBC-Go Apps	23	39	11
P1 - Critical	IBC-Go	10	10	10

C – Raw Data: Time to Close By Team by Month

Month Opened	Team	avg Days to Close	max Days to Close	min Days to Close
2023-08	Comet BFT	28	28	28
2023-08	Cosmos Hub / Gaia	70	70	70
2023-08	Cosmos SDK	22	38	9
2023-09	Comet BFT	6	6	6
2023-09	Cosmos Hub / Gaia	61	61	61
2023-09	Cosmos SDK	34	64	3
2023-09	IBC-Go	0	0	0
2023-10	CosmWasm	50	50	50
2023-10	Ledger Cosmos	26	26	26
2023-10	PFM, Horcrux, IBC-Go Apps	18	18	18
2023-11	Cosmos Hub / Gaia	38	38	38
2023-11	Cosmos SDK	26	26	26
2023-11	IBC-Go	37	42	32
2023-11	PFM, Horcrux, IBC-Go Apps	31	31	31
2023-12	Cosmos SDK	38	83	2
2024-01	Comet BFT	2	3	2
2024-01	CosmWasm	16	19	12
2024-01	Cosmos SDK	14	32	0
2024-02	Comet BFT	13	13	13
2024-02	CosmWasm	1	1	1
2024-02	PFM, Horcrux, IBC-Go Apps	34	34	34
2024-03	CosmWasm	16	28	4
2024-03	Cosmos Hub / Gaia	65	65	65
2024-03	IBC-Go	10	10	10

2024-04	Comet BFT	17	17	17
2024-04	CosmWasm	81	81	81
2024-04	Cosmos SDK	26	35	16
2024-04	IBC-Go	23	23	22
2024-05	Comet BFT	57	57	57
2024-05	Cosmos SDK	29	41	5
2024-05	IBC-Go	12	18	5
2024-06	Comet BFT	28	28	28
2024-06	Cosmos SDK	10	15	7
2024-06	IBC-Go	17	31	11
2024-07	CosmWasm	21	33	9
2024-07	Cosmos SDK	23	23	23
2024-07	PFM, Horcrux, IBC-Go Apps	39	39	39
2024-08	Comet BFT	22	22	22
2024-08	CosmWasm	23	31	12
2024-08	Cosmos Hub / Gaia	7	14	4
2024-08	Cosmos SDK	10	28	1
2024-09	Comet BFT	4	9	1
2024-09	CosmWasm	1	1	1
2024-09	Cosmos Hub / Gaia	17	17	17
2024-09	Cosmos SDK	3	4	1
2024-09	IBC-Go	3	3	3
2024-09	PFM, Horcrux, IBC-Go Apps	11	11	11