polygon

Christopher von Hessert

VP, Security @ Polygon Labs

@cvhessert

Effective Product Security: Lessons from years of bug bounties and audits

polygon

Product/Application Security is a ~~checkbox~~ process

A product's risk decreases with time & work

polygon

“The process”

Idea & Design	Development	Testing / QA	Deployment	Live
We get to play devil's advocate	***Don’t worry, we won’t bother you***	***Ok, let’s make sure this is ok***	***“Dress me slowly, I’m in a hurry”***	***We’ll keep a eye on things…***
What if …?	CI Pipeline	Peer Reviews	Rollback Plan	Bug Bounty
-	-	-	-	-
Risk Assessments	Security Scanners	Hardening	Processes	Monitoring
-	-	-	-	-
Threat Modeling	Developer Tools	Internal Testing	Checklists	Incident Response
-	-	-	-	-
Architecture Review	Dependency Checks	External Assessments	Simulations	Security Updates
		-		

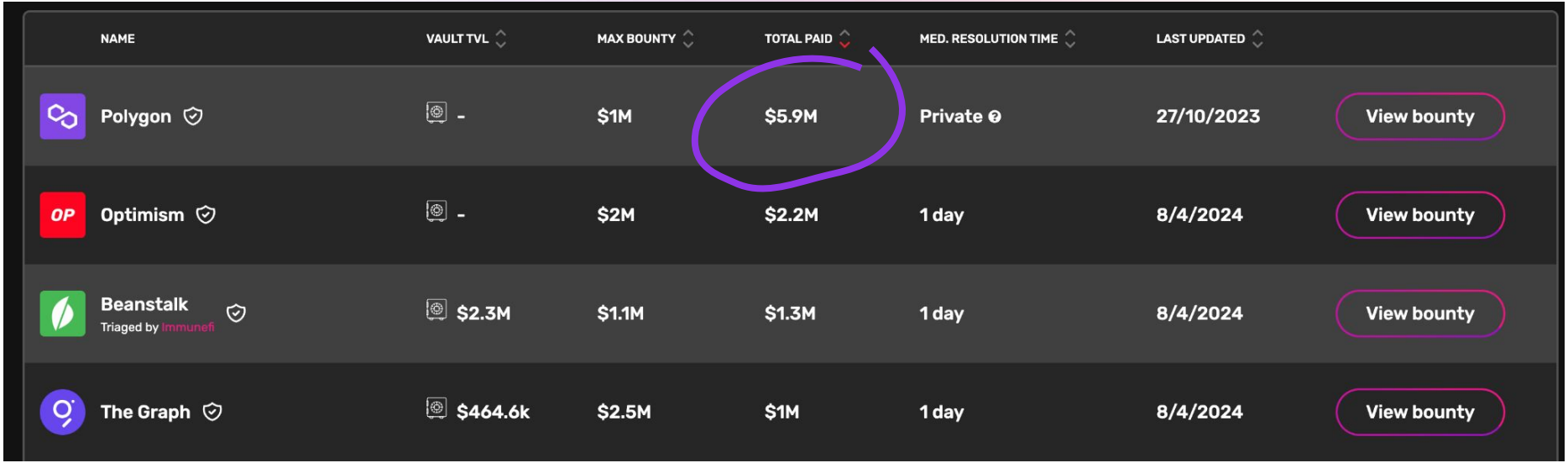
polygon

Polygon's Bug Bounty Programs

security@polygon.technology

polygon

Polygon POS #1 in Total Paid



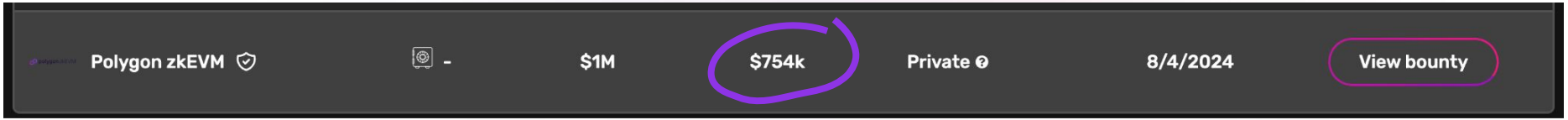
NAME	VAULT TVL	MAX BOUNTY	TOTAL PAID	MED. RESOLUTION TIME	LAST UPDATED	
Polygon	-	$1M	$5.9M	Private	27/10/2023	View bounty
Optimism	-	$2M	$2.2M	1 day	8/4/2024	View bounty
Beanstalk Triaged by Immunefi	$2.3M	$1.1M	$1.3M	1 day	8/4/2024	View bounty
The Graph	$464.6k	$2.5M	$1M	1 day	8/4/2024	View bounty

Live since September 2021

Spent $2M+ in Audits

polygon

Polygon zkEVM

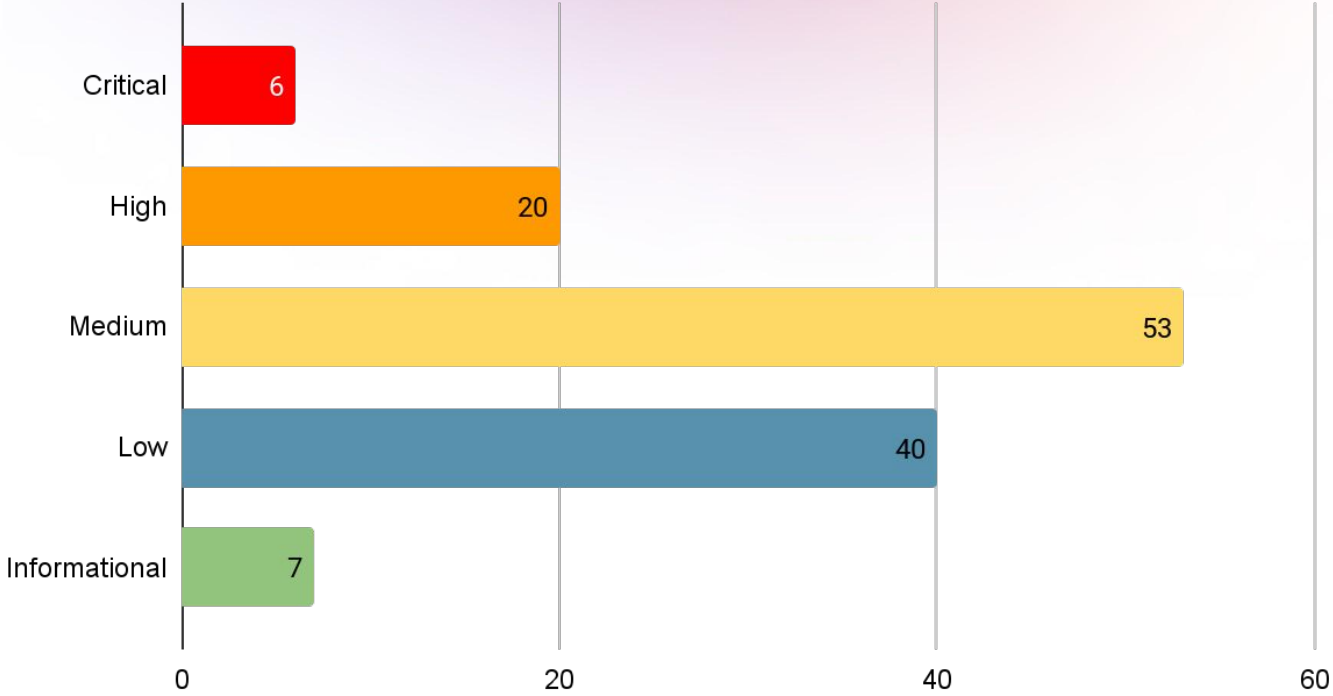


Live since March 2023

Spent $2M+ in Audits

polygon

Reports Paid by Severity since 2022



Disclaimer

These are my personal thoughts and opinions and do not represent those of Polygon

Start a bug bounty program asap, even before your product is live

As simple as bugs@acme.xyz

Setup a website: https://acme.xyz/bugbounty

Use a Google Form, Jira, etc

You can pay with your token, swag or just a public kudos **(just make that clear!)**

For Hackers: you have a better chance to get a direct consultancy deal

** These are my personal thoughts and opinions*

Scope your assets properly

Don’t

- https://github.com/acme/*
- https://acme.xyz/*

Do

- https://github.com/acme/smart_contracts/**commit/5fbd35ba9cdc8a07bf32d81d6d1f4ce745feabd6**
- https://github.com/acme/smart_contracts/**releases/latest**
- https://acme.xyz/apiv2/**swagger**

** These are my personal thoughts and opinions*

Learn how to score the severity of a report

Impact \ Likelihood	Very unlikely to happen	Unlikely to happen	Possibly could happen	Likely to happen	Very likely to happen
Catastrophic consequences	Moderate	Moderate	High	Critical	Critical
Significant consequences	Low	Moderate	Moderate	High	Critical
Moderate consequences	Low	Moderate	Moderate	Moderate	High
Low consequences	Very Low	Low	Moderate	Moderate	Moderate
Negligible consequences	Very Low	Very Low	Low	Low	Moderate

Severity of a Bug Bounty reports != Severity in a Audit Report

USE CVSS

https://gitlab-com.gitlab.io/gl-security/appsec/cvss-calculator/

** These are my personal thoughts and opinions*

Other thoughts…

Don’t set payout ranges, but if you do, make sure you communicate how that works

💎

Managed Triage? You can probably triage faster than any external team, but if you have a big program and not enough time & $$, may be worth it

💎

Don’t forget to disclose confirmed issues to others using your code before going public with it

💎

Disclose the report after its fixed, work with the Hacker on this!

💎

Mediations are not always fair (both ways) / Conflict of Interests

💎

Don’t just accept the severity set by the Hacker / Organization - Challenge why!

** These are my personal thoughts and opinions*

On Audits & Competitions…

Audits are very subjective (automated, manual, etc). Ask the methodology used.

Are you investing? Review the scope, methodology and compare to what's live

Audits are a point in time assessment, web3 moves fast, are you ready to pay for every big change?

Don’t get a audit, get a security review of your development process first

Hire a part time Security Engineer instead (he will know how & what)

Audit != PenTest: Don’t forget about your Website, DNS, GitHub repo, etc

Aren’t competitions just a time-boxed Bug Bounty?

** These are my personal thoughts and opinions*

This presentation

https://bit.ly/bugandaudits

Security for Web3
(Dummy version)

http://bit.ly/w3sec

Thank you!

@cvhessert on