Coinbase Loves Bug Bounties

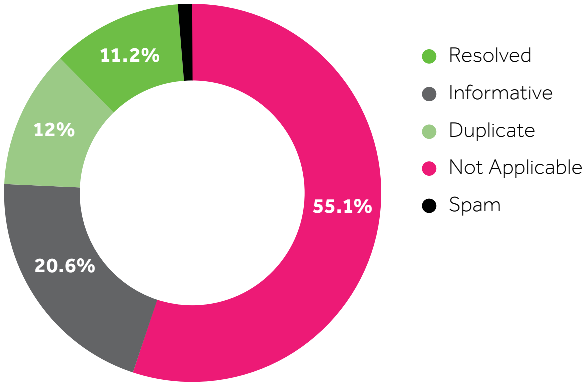
By: Philip Martin, Director of Security, Coinbase
Originally published on coinbase.com

Coinbase loves bug bounties. We think they fundamentally change the economics of vulnerability reporting. Instead of a researcher facing a choice between using a vulnerability themselves, selling a vulnerability to 3rd parties or giving a vulnerability away for free, bounties present a good, legal, risk-adjusted return for the time invested by a researcher.

Bounties de-criminalize the actions of good-faith security researchers, while still forbidding malicious hacking. Bounties help grow the next generation of security talent. We love bounties so much that we've decided to expand our bounty payouts and join a slew of other bounty-loving companies in HackerOne's Hack The World program.

Coinbase has operated a bug bounty since the beginning of the company in 2012. We started with an email address and the coinbase.com/whitehat page. We paid out rewards in bitcoin (obviously). This scaled poorly. Fortunately for us, HackerOne showed up on the scene at just the right time, and we moved onto the platform in March of 2014. Over the last five years we've seen a lot of the good and bad sides of the bug bounty world. We've paid out $176,031 in bounties to 223 researchers across 346 valid reports out of a total of 3101 reports submitted. We've disclosed 73 of the valid reports, and have a general policy of disclosing when requested.

So, why make changes? We take security incredibly seriously (if you don't in this space, you end up in the Blockchain Graveyard). We regularly review every aspect of our security program, and when we looked at our bug bounty this time around we were struck by two gaps:



To date, we've not really explored bounty promotions as part of our overall program. We want to see if creatively applied promotions can help us increase report quality and researcher engagement. To that end, we will be participating in HackerOne's Hack The World program and running a promotion specific to participants in that program: we will pick the top 3 most impactful bugs submitted as part of Hack The World and award them an additional $10,000, $7,500 and $5,000 for first, second and third place. "Most Impactful" will be judged by the Coinbase security team on a combination of bug severity, system criticality and report quality.

When we took a look at bounty payouts industry-wide, we felt the need to rebalance some of our bounty payout tiers to remain top-of-market. Effective immediately for all new bounty submissions (that is, submissions originally dated after 4 PM, 18 Oct 2017 (UTC)), we will use the following payout guidelines:

- Remote Code Execution: $50,000
- Significant manipulation of account balance: $10,000
- XSS/CSRF/Clickjacking affecting sensitive actions: $7,500
- Theft of privileged information: $5,000
- Partial authentication bypass: $3,000
- Other XSS (excluding Self-XSS): $1,000
- Other vulnerability with clear potential for financial or data loss: $1,000
- Other CSRF (excluding logout CSRF): $250
- Other best practice or defense in depth: $100

We're thankful to all the security researchers who have worked hard to find and report vulnerabilities in Coinbase. If you're interested in helping keep Coinbase the most trusted place to buy and sell digital assets, then take a look at our bug bounty program, sign up for Hack The World or apply to one of our open security positions!

coinbase *Published on October 18, 2017*