bugcrowd

Crawl, Walk, Run: How Twilio Has Successfuly Harnessed the Power of the Crowd for Years

By working closely with the security research community through a private and public bug bounty program, Twilio has augmented their existing testing efforts and have received deep engagement and high-quality results.

Improving Product Security with the Crowd

Twilio, the cloud communications company out of San Francisco, CA, is an early adopter and innovator in the cybersecurity domain. Although they have consistently prioritized Product Security, they wanted to concentrate their efforts on the areas of greatest risk. To help augment their internal and external testing efforts, they turned to the crowd to start uncovering more vulnerabilities and learn from those findings.

Coleen Coolidge, Sr. Director, Information Security, Twilio

"By adding the power of the talented researcher community to our Product Security program, we've learned a lot about how people outside the company think about our products, additional scenarios where products can be at risk and what else we could do to protect our products. We've used this information to put a sharper focus on the areas of greatest risk, which has been invaluable to us as we scale."

twilio

About the Twilio Program

https://bugcrowd.com/twilio

Launched: March 22, 2014

Type: Private to Public

Scope: Twilio web properties, APIs, and endpoints

Rewards: Up to $5000 per bug

Total submissions: 1200+

Submitting Researchers: 500+

Paid out: $50,000

Crawl, Walk, Run Approach

Not only have they leveraged the global crowd of independent security researchers through Bugcrowd for over two years, but they have utilized the model in a variety of ways and have benefited from their consistent engagement.

They started with a private program, moving towards a public program, and have tweaked their scope and rewards as they've gone:

March 22, 2014

Twilio launched their private program, offering rewards initially up to $2000 per bug. By interacting with just the most skilled and trusted pool of researchers, Twilio was able to put processes and standards in place, make internal cultural changes, and ease into a more collaborative security testing model.

Learn more about private programs >

December 2, 2014

Less than nine months after launching their private program, Twilio transitioned to a public program. With their initial success and positive experience with the private program, their team felt ready to open participation to include a bigger, more diverse pool of testers.

Learn more about public programs >

November 25, 2015

They upped the ante on their program, increasing their reward payouts to $5000, making them a higher paying out organization. To boost engagement, and incentivize more critical bugs, this update has proved successful in increasing submission volume and quality.

Learn more about reward ranges >

bugcrowd

TWILIO CASE STUDY

Bug Bounty Program Results

Throughout the lifetime of their program with their “crawl, walk, run” tactic, they have been able to maintain strong engagement over time.

1200+
TOTAL SUBMISSIONS
As of the end of 2016, the Twilio program has received over 1200 submissions from over 500 researchers coming from **64 countries**.

3.28
AVE. PRIORITY
They have received a very healthy amount of valid bugs, which translates to an average priority across submissions of 3.28.

$50K
TOTAL PAID OUT
Payouts have gone to researchers from Portugal (37%), India (26%), United States (13%), and Great Britain (9%) with an **average payout of $475.**

Thanh Nguyen
Location: Vietnam
Acceptance Rate: 100%
Priority: 3.06

“They play very fair. In my opinion, what makes a bug bounty program great is not how many bugs they have, it is how they handle their bugs. When you play fair, all researchers will be happy to join your program.”

Robin Ooklay
Location: India
Acceptance Rate: 94%
Priority: 3.94

“It’s quite a pleasure to work at Bugcrowd and their bounty programs. Twilio is one of the great programs among them, quick response time, understanding the priority and severity of issues, fixing them instantly and rewarding the hunter suitably. ”

Working Closely With The Crowd

Through their private and public bug bounty program, they have strengthened their relationship with the researcher community and received steady contributions with many top researchers. This collaboration has been successful, as proof of the depth and breadth of their results and strong engagement across the researcher community.

This is one of the most important aspects of their bounty program, and their commitment to maintaining a healthy relationship with researchers has been noticed. **At left are two top contributors on why they appreciate the Twilio program.**

Key Learnings

In addition to receiving high-quality results through their bug bounty program, Twilio has learned a lot from working with the security researcher community.

Davit Baghdasaryan, Product Security Lead, Twilio

“Our bug bounty plays a key role in our Product Security program. It has helped us to define and shape this program. We are getting access to a large talent pool who are incentivized to test, find and report security vulnerabilities on our platform. This is a win-win situation for everyone.”

With Bugcrowd’s support, their bounty program has helped them meet their overall Product Security needs and goals:

- Crowdsourced testing has improved upon their existing Product Security initiatives, finding additional unknown and high-value vulnerabilities and an incredible return on investment.
- The additional layer of triage and validation provided by Bugcrowd has allowed them to increase their vulnerability finding capabilities while freeing up resources and allowing their security team to focus on other areas of the business.

Their success is indicative of their commitment to Product Security, and they will continue to evolve and maintain their bug bounty program.

To learn more about our bug bounty solutions, visit bugcrowd.com/demo.