QUALCOMM'S ALEX GANTMAN ON BUG BOUNTIES

Published on 22 June 2017

Qualcomm | hackerone

Their silicon powers today's hottest smartphones and fastest wireless networks, but they use HackerOne to power their bug bounty program.

Smartphones aren't the only places you'll find cutting-edge wireless components. If you're using any connected device, chances are it's using Qualcomm technology.

From smart refrigerators in your kitchen to cardiac monitors in a hospital, Qualcomm's processors, modems, and other wireless technologies are powering the world of connected devices. But as the number of those devices continues to explode—to as many as 20 billion by 2020—the focus on security becomes more prominent.

But since Qualcomm's technology isn't the end product, it's sometimes difficult to determine the root of a device's vulnerability. That's why Qualcomm relies on the cleverness of the hacker community to help improve the security of their products.

We recently caught up with Alex Gantman, vice president, engineering, Qualcomm Technologies, Inc and asked four questions about Qualcomm's approach to bug bounties and hacker-powered security.

Q. From your personal experience, what were some of the considerations and challenges your company encountered when initially creating a bug bounty program—things perhaps other companies considering bug bounty programs will want to prepare for? What do you see as the biggest barrier to entry at this point that still might make certain companies hesitate to start their own?

We understood very early on that working with the security research community is an integral part to continuously improve the security of our products. We've been lucky enough to work with a top-notch researcher community. We recognize that conducting security research often requires investing a large amount of time and skill in order to make an impact, and we definitely appreciate the hard work and effort that external security researchers have put in.

> *That's why we wanted to find a way to show our appreciations towards the researchers who have contributed.*

In general, for any institution to have a vulnerability rewards program, a.k.a. bug bounty, it is a prerequisite to have a well-oiled incident response process that is able to handle large amount of incoming vulnerability reports. An established secure development life cycle within the organization is also needed to turn reactive work into proactive vulnerability prevention and early detection.

Also in large organizations such as ours, having internal teams such as engineering, communications, and legal all on the same page is very important; but having support from C-suite executives is crucial. Fortunately, we lined all that up in the early planning phase at Qualcomm.

The biggest consideration we have, and this probably true for all silicon chip providers,is that our products are the components other device makers use to create their products. In other words, security researchers first analyze devices made by our customers, then must conduct further research to separate what might be a Qualcomm issue.

> *We would like to make it easier for these researchers to directly look into our products.*

With all the challenges and considerations mentioned above, it's no surprise that Qualcomm is the first among silicon chip providers to launch a vulnerability rewards program.

It's worth mentioning here that our program is a private one by invitation only. The reason we started with a private one is multi-fold. First, we wanted to keep the noise low. Any public bug bounty program will have quite large number of unrelated or out-of-scope submissions. These reports still require manual work to sift through.

But by working with talented and trusted security researchers, we can minimize the noise and increase our own efficiencies. Second, embedded device security is a specialized area within the whole spectrum of information security. Through the years of working with the researcher community, we have collected a list of top notch researchers that have specialized in our area.

By working directly with them, we are able to get high quality reports. Also, we can provide more direct support to this group of researchers. As I mentioned before, it's often challenging for security researchers to figure what portion of the hardware and software is coming from Qualcomm when they analyze a commercial device.

Working with this group of researchers directly, we can guide them to focus on specific areas where Qualcomm can assist. Third, our invitation list is not capped. Whenever we identify new talented security researchers in our area, we invite them to join our program to help us protect customers.

Q. How does the existence of gray-hat external bug bounty programs influence the need for companies to start their own legit program? In other words, if a company that finds bugs and sells them to governments or the highest bidder is encouraging hackers to sniff out flaws in certain companies' websites or software, does that put pressure on this company to create their own responsible disclosure program that offers rewards that can compete with these gray hat services? Was this a consideration when your company started the program?

In our view, vendors who already have a bug bounty program or are preparing to have one should not target the underground or gray market bounty programs. Some published data suggest that vulnerabilities, especially critical ones that allow remote code execution, have a much higher price tag on the third-party bounty market compared to vendors' own rewards programs.

> *At Qualcomm, the security researchers we have worked with are not motivated by financial gains. Instead, they want to help us make our products more secure in order to protect more people.*

One simple but important thing we've learned from working with security researchers over many years is that people like to work with people. When researchers report an issue, our security team works diligently to address them in addition to interacting with the researcher. This communication is rewarding and enlightening, and you cannot get that from third-party bug bounty programs.

> *That's why for every submission, we ask our security engineers to reply to the researcher, talk with them, and provide periodic updates.*

This communication, combined with a rapid response process and a rewards program to recognize researchers' contributions, are certainly effective ways to establish mutual respect and trust between security researchers and companies.

Q. Anecdotally or metrically, explain how you've benefited from your bug bounty program in terms of identifying an especially critical vulnerability, stopping an exploit, etc. Any statistics you can share re: how much you've given out in rewards or how many vulnerabilities have been detected in total, average per month/year, etc.?

It has been three months since the official launch of Qualcomm's vulnerability rewards program. Overall, we've received some great reports, and we are pretty happy with how it is going so far. For every valid issue reported, we do what we call gap analysis to figure out what we can do internally to catch similar issues during our development stage.

So essentially, **we view the findings from these very skilled researchers as part of the feedback loop to help us improve our secure development life cycle internally. It's quite valuable input.** In the first three-month period, we've given out around $80,000 in rewards.

Q. Offer a prediction or two on how bug bounty programs will evolve or grow based on current discernible trends.

We believe there will be more bug bounties programs offered by vendors down the road because it is an effective way to find vulnerabilities that otherwise may go unnoticed. It also helps vendors to connect with security researchers and provide valuable input to internal security work. Vulnerability rewards program really should be viewed as an extension of a company's product security initiatives.

> *In today's day and age with security so highly valued, we are seeing companies pay more attention to the security of their products.*

Consumers are becoming more aware of the security of the devices they depend on every day, be it a smart phone, home router, or connected home camera. In such a connected world with so many products to choose from, security is becoming one of the leading differentiators when it comes to the purchase decision.

With these market forces in play and combined with pressure from regulators, **we expect more companies to establish their own security programs such as a secure development lifecycle.** In these companies, it will become natural to decide if a bug bounty program makes sense to implement.

A certain healthy margin of profit is needed so companies can continue investing in and improving their security programs. This investment in security will be quite challenging for some of the IoT device segments with low cost and low margin business models.

But whether a small company or a large one like Qualcomm, we have found that efforts to protect customers more than often pays off in the end.

Qualcomm and over 800 other organizations work with HackerOne to secure their products and services. Talk to us today to learn more and start your own program.

HackerOne Has Vetted Hackers For Hundreds of Organizations Including:

GM · Starbucks · Lufthansa · European Commission · Twitter · Spotify · U.S. Air Force · airbnb · yelp · LendingClub · U.S. Army · Google Play · New Relic · Nintendo · Adobe · Dropbox · Snapchat · YAHOO! · coinbase · shopify · slack

With Over 900 Customers, More Companies Trust HackerOne Than Any Other Vendor