bugcrowd

Aruba Networks Commits to ONGOING PRIVATE BUG BOUNTY FOR BETTER DEVICE SECURITY

PROGRAM DETAILS

Launched: October 2014

Type: Ongoing Private Bug Bounty Program

Scope: ClearPass Policy Manager, AirWave, Aruba Instant, Access Points, ArubaOS running on devices and Aruba Virtual Intranet Access Client

Rewards: $100 – $5,000 per vulnerability

Taking Advantage of the Crowdsourced Security Model, Aruba Networks is committed to building smarter networks and enabling secure connectivity for mobile and IoT.

As Aruba scaled its operations to meet demand, it knew that product and application security needed to be prioritized. Aruba brought on an all-star security team, carried out multiple expensive third-party testing engagements and even hired some independent security researchers to freelance. Even still, they needed more eyes looking at their attack surface and turned to Bugcrowd to augment their existing efforts.

After evaluating their current testing capabilities and organizational goals, Aruba decided to harness the collective power of human intelligence through Bugcrowd's more focused Ongoing Private Bug Bounty Program.

Program Highlights

With the Ongoing Private Bug Bounty Program, Aruba has been able to tailor their testing pool based on specific skill sets, have more direct communication with a smaller group of testers, while still taking advantage of the crowdsourced model. After over three years of utilizing the crowd to test their products and applications, Aruba has seen tremendous results, have positioned themselves as thought leaders in application security, and have seen continued traction in their programs.

Aruba, one of the first organizations to utilize the Ongoing Private Bug Bounty to test hardware, has been recognized by the security research community for its commitment and innovation. To provide Aruba Networks with increased privacy and control, Bugcrowd segmented and invited 100 of the top vetted and trusted researchers to participate in its Ongoing Private Bug Bounty Program in early 2014.

Because of its consistency, the Aruba program has retained astounding traction over three years.

aruba NETWORKS

Since 2014, Aruba has successfully leveraged Bugcrowd's most skilled sand trusted researchers to increase security of its devices.

Jon Green,
Vice President & Chief Technologist of Security

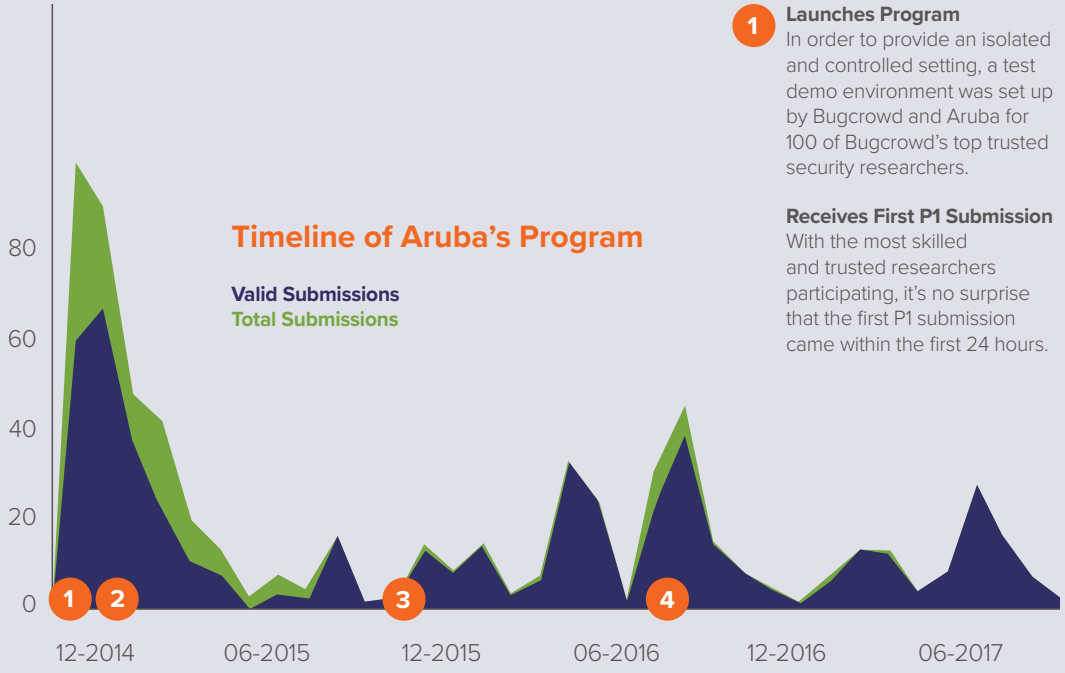
"We have products that cover a wide variety of applications that utilize various technologies, so we need security testing that can cover all those areas. Bugcrowd's Ongoing Private Bug Bounty is the best way to get the coverage. Of course, this entire line of thinking starts with the premise that we think product security is of the utmost importance – we want to find the problems before someone else does so that we can help keep our customers secure."

307
TOTAL VALID SUBMISSIONS

2.35*
AVERAGE VULNERABILITY PRIORITY

$206,550
TOTAL PAID OUT

*average priority is based off a scale of 1, being highest, to 5 being the lowest.



1 **Launches Program**
In order to provide an isolated and controlled setting, a test demo environment was set up by Bugcrowd and Aruba for 100 of Bugcrowd's top trusted security researchers.

Receives First P1 Submission
With the most skilled and trusted researchers participating, it's no surprise that the first P1 submission came within the first 24 hours.

2 **Receives First 100 Submissions**
The Aruba Ongoing Private Bug Bounty Program garnered high traction within the first month from many top researchers such as Duarte Silva.

3 **Adds additional 100 researchers**
To boost engagement and broaden the testing pool, Aruba added additional researchers to the program, including Luke Young.

4 **Receives 500th Submission**
Because of their consistency and transparency, Aruba has received consistent attention from the researcher community over the last few years.

The Value of an Ongoing Private Bug Bounty

Ongoing Private Bug Bounty Programs are ideal for testing targets that are not already publicly accessible such as systems on staging environments, applications that require credentials or logins, and even physical devices. To gain access to private programs, researchers are vetted, verified and trusted through participation in public programs.

"We decided to run a Ongoing Private Bug Bounty Program in order to get access to a wide variety of highly skilled security testers. Hiring security researchers is very difficult in today's market, and even if you can find one, chances are good that person will be a specialist in only one or two areas."

Jon Green, VP & Chief Technologist for Security, Aruba Networks

Working Closely with the Researcher Community

Working with the security researcher community is one of the greatest value-adds of the Ongoing Private Bug Bounty Program for Aruba. The team have exhibited immense dedication to the community with a fast response time, consistent communication, and a documented coordinated disclosure policy. These factors have helped the Aruba team gain valuable testing efforts from some of the top bug hunters in the world.

Researcher Profiles

Luke Young, United States

Acceptance Rate: 100%

Priority: 2.34

"Crowdsourced security programs depend on an incredible amount of trust between all parties involved and Aruba has done a fantastic job of building that trust and at the same time a professional relationship with their researchers. Because of that open communication and the relationship I've been able to build over time, Aruba Networks is my above and beyond my favorite program to work with."

Learn why hundreds of companies have turned to Bugcrowd.

www.bugcrowd.com/get-started

Bugcrowd.com
Sales@Bugcrowd.com | (888) 361-9734