bugcrowd

BUGCROWD ENABLES HP TO DELIVER THE MOST SECURE PRINTERS

HP Partners with Bugcrowd on First-of-its-Kind Bug Bounty Program

How HP Ensures the Most Secure Printing

Internet of Things (IoT) security has gained a lot of visibility over the last couple of years. Printers, arguably the most common IoT devices on the market, touch and store some of the most sensitive data and yet these devices are often left out of the organization's security policy. This is why security is a core pillar of HP's product strategy.

To achieve a high level of security, HP has built security into every product and device from the beginning — setting up mechanisms to detect potential malware attacks, adding protections for data at rest and in transit, as well as protecting documents as they flow through the print subsystem and the device.

From risk and threat analysis, static code analysis and vulnerability scanning and penetration testing, HP performs comprehensive security testing on every product before it goes out. HP has also provided behavioral anomaly detection in all Enterprise devices. With best-in-class defensive strategies in place HP wanted to take their security strategy one step further with a bug bounty program.

HP Turned to Bugcrowd

HP has always been committed to partnering with key security leaders in the industry. When it came time to selecting a crowdsourced security partner, the company chose Bugcrowd. With Bugcrowd's private bug bounty program, HP incentivizes an elite, trusted Crowd of security researchers to find critical issues or vulnerabilities in its products. Given the difficulty of finding these obscure vulnerabilities the bug bounty program is key.

About the HP Inc. Program

Launched: 2018

Type: Private bug bounty

Scope: Private

Rewards: Up to $10,000

Average Priority: 2.34

"Security is critical at HP. It's all about the three Ds, protecting customer devices, data, and documents."

"We looked at the bug bounty program as a key mechanism for taking our security posture to the next level. By leveraging a community of security researchers to find some of those obscure issues no one else has found. This is the message that convinced our executives to support the program."

Shivaun Albright, Chief Technologist, Print Security, HP

Private bug bounty programs offer organizations like HP the opportunity to utilize the power of the crowd — volume of testers, diversity of skill and perspective and competitive environment — in a more controlled and stringent environment. In fact, the majority of programs run on Bugcrowd are private — nearly 80%. Private programs are limited to vetted and trusted researchers, giving companies the power to control what is tested and how it's tested. This type of program is a great entry point for anyone looking to start their first bug bounty program or introduce testing on a new asset — it offers significant breadth and depth of coverage without overwhelming your security and development teams.

Using proprietary algorithm for matching researchers to programs, combined with extensive verification checks, Bugcrowd distinguishes its Bugcrowd Elite — Bugcrowd's private Crowd of skilled and trusted security researchers.

The Elite Crowd is comprised of the top researchers, measured in two key areas:

Skill — A standard of high-impact submissions, averaging only high and critical submissions across a range of specific attack surface areas.

Trust — Proven trust through ID verification and success working on private programs for top customers.

By adopting this crowdsourced security approach, HP gained access to the Bugcrowd Elite to identify and patch issues they would not have detected through defensive methods alone.

Program Results

HP very quickly realized the value of the bug bounty program, seeing obscure quality findings come in through Bugcrowd. Ultimately, the program helped HP better protect its customers' data and infrastructure.

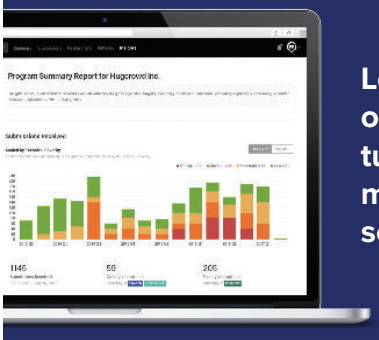
With the ongoing private bug bounty Program, HP has been able to tailor its testing pool based on specific skill sets, has more direct communication with a smaller group of trusted and skilled testers, while still taking advantage of the crowdsourced model.

"Bugcrowd has expanded our approach to vulnerability testing. Bugcrowd has provided us with a clearer understanding of the hackers' mentality, by bringing all the key parties together in a common, collaborative way. That is a key benefit that we've seen working with Bugcrowd."

"Whenever you invest money, you need to consider the return on investment. So for every dollar we spend, we ask what is the benefit we are going to gain? The bug bounty program is a highly cost-effective way to identify obscure vulnerabilities."

"Anytime we find an obscure issue in our products it is an 'Aha' moment. It is a learning opportunity and we start a dialogue with the researchers, to understand what methodologies they used, what tools they used to find the particular issue, and then we incorporate those key learnings into our own security testing so that we can make sure similar issues do not occur in the future."

Shivaun Albright, Chief Technologist, Print Security, HP



Learn why hundreds of companies have turned to Bugcrowd for managed crowdsourced security programs.

www.bugcrowd.com/get-started

Bugcrowd.com
sales@bugcrowd.com | (888) 361-9734