ownCloud and HackerOne Collaborate for Better Security

Problem

ownCloud is a company and open source project that helps customers access and share their files and personal data from any device. Over 8 million users worldwide use ownCloud to keep their data secure on devices and in the cloud. Thanks to contributors, ownCloud received security vulnerability reports regularly. They even received customer penetration test results, but were concerned when some of those pentests failed to find any vulnerabilities. Knowing that all software contains vulnerabilities, ownCloud wanted more and higher-quality vulnerability reports than existing contributors and penetration testing were providing.

> *"The third party inspection of code adds a layer of confidence to ownCloud's over 8M users and administrators. Enterprises know their deployment has undergone the rigors of ownCloud QA, their own testing, and the bounty-driven testing of security experts resulting in more secure file sharing for many environments."*
>
> - Matt Richards, VP of Products & Markets, ownCloud.

ownCloud decided that by getting more eyes on its software, they could discover and address more issues. To do so, ownCloud launched its own vulnerability coordination program in 2012. Despite finding more valid vulnerabilities, the security team also found the program too noisy, generating a high rate of invalid and

out-of-scope reports.

CEO Markus Rex knew from his experience as General Manager of SUSE Linux that more eyes -- and the right sets of eyes -- could further improve ownCloud's security. He asked Lukas Reschke, Head of Information Security at ownCloud, to figure out how to get the hacker community to focus on ownCloud.

Solution

In 2015, ownCloud selected HackerOne to be their vulnerability coordination partner based on trust and an open approach to security research. HackerOne provided straightforward, no-nonsense answers to ownCloud throughout the evaluation. Also, HackerOne's approach to security research - encouraging openness - was well aligned with ownCloud's open source mission. They first began by launching a small-scale private program in order to get used to the quality and quantity of reports. After getting settled in, ownCloud then stress-tested their own response capabilities by inviting a

whopping 600 hackers. They wanted to ensure their team could consistently collaborate with a large number of hackers at scale, identify important reports from among a larger volume of incoming reports, and maintain quick response times to keep hackers engaged and motivated. After successfully managing the spike within their private program, ownCloud opened their program to the public and offered a bug bounty for vulnerability reports.

Results

Within two weeks of launching its public program on HackerOne, ownCloud received more than 200 reports. They quickly resolved many of these, and awarded bounties for two particularly significant vulnerabilities.

Time to receive 100 vulnerability reports:

Before HackerOne - 150 days
After HackerOne - 7 days

Surprisingly, one of these vulnerabilities had been caused by code written and deployed in 2004, a full twelve years prior. "Without the breadth of HackerOne hackers investigating ownCloud, we would not have found that vulnerability," said Reschke.

The greatest benefit ownCloud gained by using HackerOne was saving time. Rather than the large number of poor reports that they spent time fielding prior to using HackerOne, Reschke and his team could now focus their time reviewing and fixing the most important vulnerabilities, such as this **Information Exposure report.** Inbound report quality continues to increase as the 100 consistently contributing hackers on their program gain intimate familiarity with ownCloud's software. Additionally, ownCloud's signal (percent of valid reports among all reports received) has reached a record-high over the last two months, exceeding the HackerOne platform average for all public programs. ownCloud is getting more high-quality reports than ever before.

And they're not done yet. A few months after launch, HackerOne customers typically experience an expected decline in submissions after the initial wave of easy-to-find vulnerabilities have already been reported. To maintain the volume of discovered vulnerabilities, ownCloud has ideas to keep volume up. "We plan to increase the size of our bug bounties," said Reschke. "I am confident that HackerOne's community of hackers will continue rising to the challenge."

