6.5 Independent Discovery

If one person can find a vulnerability, somebody else can, too. Andy Ozment [1] showed that "vulnerability rediscovery occurs 'in the wild' and that it is not particularly uncommon." Finifter and colleagues, reviewing a dataset of Chrome vulnerabilities, identified 15 out of 668 (2.25%) that had been independently discovered by multiple parties [2]. They go on to mention similar rates for Firefox vulnerabilities. Ablon and Bogart [3] studied a stockpile of zero day vulnerabilities, estimating that "after a year approximately 5.7 percent have been discovered and disclosed by others." Herr and Schneier [4] find browser vulnerabilities having rediscovery rates between 11% and 20% annually for the years 2013-2015. For Android vulnerabilities during the 2015-2016 timeframe, they found an annual rediscovery rate of 22%.

What is to be done when the CVD process is underway for a vulnerability, and a seemingly independent report of the same vulnerability arrives? One approach is to accelerate the disclosure timeline, possibly disclosing immediately. This approach assumes that if a vulnerability has been found and reported by multiple individuals acting independently, then it must be an easy vulnerability to find. This in turn implies that others who haven't reported it may also be aware of its existence, thereby increasing the likelihood of its availability to adversaries.

While we find this to be a reasonable conclusion, CVD participants should be wary of duplicate reports that are not independent. Truly independent discovery does yield some indication of the difficulty of finding a vulnerability. But vulnerability finders and security researchers talk to each other, and they sometimes hunt in the same places. An announcement of interesting vulnerabilities in a product can spur others to turn their attention and tools to that product. Even a casual "I've been looking at product X and found some interesting things" can put someone else on the hunt for vulnerabilities in product X. Any judgement of independence should consider the degree to which there is community interest in a product. As the popularity of products wax and wane through their lifespan, so too will security researcher attention.

An example of a coordination failure occurred during the vulnerability disclosure of Heartbleed. Two organizations, Codenomicon and Google, both discovered the vulnerability around the same time. When the vulnerability was reported a second time to the OpenSSL team, the team assumed a possible leak and the vulnerability was quickly disclosed publicly [5]. A more coordinated response may have allowed further remediation to be available immediately at disclosure time.

Even more insidious is a phenomenon we've observed in bug bounty scenarios. Because they pay for reports, bug bounties can unintentionally provide incentives for finders to share their reports with others prior to reporting, allowing multiple individuals to report the same bug, and potentially share in a larger payout. CVD is a social game: as such, its incentives affect participants' behavior.

Rather than prescribing a single rule that independent discovery should immediately trigger release of the vulnerability information, we suggest that CVD participants discuss the implications of rediscovery on a case-by-case basis in order to decide the best course of action for the particular case.

< 6.4 Intentional or Accidental Leaks | 6.6 Active Exploitation >

References

1. A. Ozment, "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting," in *Workshop on Economics and Information Security*, 2005.
2. M. Finifter, D. Akhawe and D. Wagner, "An Empirical Study of Vulnerability Rewards Programs," in *22nd USENIX Security Symposium*, 2013.
3. L. Ablon and T. Bogart, "Zero Days, Thousands of Nights," RAND Corporation, 2017.
4. T. Herr and B. Schneier, "Taking Stock: Estimating Vulnerability Rediscovery," 7 March 2017. [Online]. Available: https://ssrn.com/abstract=2928758. [Accessed 16 May 2017].
5. B. Grubb, "Heartbleed disclosure timeline: who knew what and when," The Sydney Morning Herald, 15 April 2014. [Online]. Available: http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140414-zqurk.html. [Accessed 23 May 2017].