6.8 Hype, Marketing, and Unwanted Attention

In the past few years we've witnessed the rise of branded vulnerabilities: Heartbleed [1], Badlock [2], Shell Shock [3], and GHOST [4]. Does having a marketing department behind a vulnerability disclosure make that vulnerability worse than others without the marketing push? Not in any technical sense, no. Instead, what it does is draw additional attention to the vulnerability—so vendors can be forced to adjust the priority of the vulnerability cases they're working on and allocate resources toward addressing whatever vulnerability is getting the hype. Are branded vulnerabilities good or bad for internet security? The only good answer is the lesson of the Taoist parable of the farmer and the horse: "Maybe." [5].

The Streisand Effect

Attempts to squash true information once it's been revealed tends not only to spread the information more widely, but also to backfire on whoever is trying to conceal it. The name comes from a case involving the removal of online photos of a famous celebrity's house [6]. The attempt to suppress the photos only drew attention to them resulting in many more people seeing them than would have otherwise.

This scenario comes up from time to time in CVD cases. Often it takes the form of a vendor trying to suppress the publication of a report about a vulnerability in its product, with some threat of legal action if the information is released. As we've discussed previously, the knowledge that a vulnerability exists in some feature of a product can be sufficient for a knowledgeable individual to rediscover the vulnerability. The legal threats usually serve to amplify the discussion of the case within the security community, which draws more attention to the vendor and its products at the same time it demotivates reporters' willingness to participate in the CVD process. Even more problematic is that when such attention comes to focus on the vendors' products, it is very likely that additional vulnerabilities will be found—while simultaneously less likely that anyone will bother to report them to the vendor before disclosing them publicly. Vendors should not underestimate spite as a motivation for vulnerability discovery.

< 6.7 Relationships that Go Sideways | 6.9 What to Do When Things Go Wrong >

References

1. Codenomicon, "The Heartbleed Bug," 29 April 2014. [Online]. Available: http://heartbleed.com/. [Accessed 16 May 2017].
2. SerNet, "Badlock Bug," 12 April 2016. [Online]. Available: http://www.badlock.org/. [Accessed 23 May 2017].
3. N. Perlroth, "Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant," 25 September 2014. [Online]. Available: https://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html. [Accessed 23 May 2017].
4. A. Sarwate, "The GHOST Vulnerability," 27 January 2015. [Online]. Available: https://blog.qualys.com/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability. [Accessed 23 May 2017].
5. A. Watts, C. Huang and L. Chih-chang. Tao: The Watercourse Way, Pantheon, 1975.
6. M. Masnick, "For 10 Years Everyone's Been Using 'The Streisand Effect' Without Paying; Now I'm Going To Start Issuing Takedowns," 8 January 2015. [Online]. Available: https://www.techdirt.com/articles/20150107/13292829624/10-years-everyones-been-using-streisand-effect-without-paying-now-im-going-to-start-issuing-takedowns.shtml. [Accessed 23 May 2017].