RSA Conference 2018

MATTERS NOW

Peer2Peer

Vulnerability Disclosure: Are we sharing too much too soon?

P2P1-W09: Vulnerability Disclosure: Are We Sharing Too Much Too Soon?

Tammy Green, Senior Principal Product Security Architect, Symantec

The number of CVEs published by the National Vulnerability Database (NVD) in 2017 increased dramatically to more than 14,000 CVEs – more than two times more CVEs than 2016. According to VulnDB, over 16,000 vulnerabilities were disclosed. Vulnerability transparency has become the norm, providing useful information to vendors as well as attackers. It is no longer clear whether publishing more vulnerability information is helping organizations to identify and remediate vulnerabilities, or whether it is enabling more attacks.

The two RSA Conference 2018 Peer2Peer sessions Vulnerability Disclosure: Are we sharing too much too soon? provided fascinating insights into how vulnerabilities are regarded and handled across multiple types of organizations.

The discussions centered around when to publish vulnerabilities and what information should be included. Overall, it seemed to be acceptable to publish vulnerabilities in open source as soon as they are discovered and a fix is available. For all other types of vulnerabilities, when/if vulnerabilities should be published depends on many factors, some of which may not be clearly specified. Spectre and Meltdown were discussed as an example of handling vulnerability disclosure badly: more people should have been involved, more care should have been used to prevent leaks, and fixes were not vetted before being released.

When the discussion shifted to publishing vulnerabilities in their own products, there was less consensus but there were similarities. Most agreed that there were too many vulnerabilities to publish all of them, so they use various techniques to identify what is important to publish. A couple of people disagreed, saying that it was far easier to publish everything. Another attendee noted that failing to announce fixes gives an attacker the upper hand. Attackers periodically review patches and updates to identify vulnerabilities that were fixed in the latest release but not communicated. An attacker can then create and deploy exploits for earlier releases. Announcing a vulnerability increases the number of people who will patch, and decreases the success of an attacker.

Early publication of a vulnerability before the fixes are published seemed reasonable only if it could provide value (e.g., a mitigation technique). Spectre and Meltdown were identified are examples of how publishing before a fix is provided can increase risk substantially.

Overall, my takeaway is that our responsibility is to do the least harm. Identifying what that means is complicated and varies between companies, product teams, and even between different vulnerabilities. Guidelines and best practices along with executive input are key to making good decisions for our organizations. As I returned from the RSA Conference 2018 this year, I have a new project to update existing guidelines and best practices for publishing vulnerabilities, and to consider a few new ones that will do the least harm.

https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all

https://vuldb.com/?archive.2017