What Happens When Vendors Self-Certify Information on Vulnerabilities in Their Products?

Tsafrir Livne

In recent years, organizations have been suffering from soaring damages due to cyberattacks that cripple business operations and impair reputation. Software vulnerabilities are often cited as a prime contributor in these incidents. Concomitantly, medical device manufacturers and auto makers issue product recalls due to the discovery of critical, life threatening vulnerabilities in their software. The U.S. Department of Homeland Security runs the CVE (Common Vulnerabilities and Exposures) project, a certified registry of vulnerability information, which serves as a prime source of information for decision-makers such as procurement and corporate risk officers. This paper evaluates how vendors influence vulnerability information. Comparing the severity of vulnerabilities certified by affected vendors with those certified by independent third parties, the former tends to be significantly lower on average. These findings are robust to different specifications and raise concerns about the quality of public information about security vulnerabilities, emphasizing the need for public discussion on the stewardship of this pivotal system.