Secure testing of Open Source Projects

Area of interest: Initial minimum requirements for testing software source code

Open source adoption in the Industry has been increasing tremendously. While Open source software is crucial for innovation and agile development, it is also important to secure its procurement and ongoing use.

Industry statistics show that there was 88% growth in application vulnerabilities over last two years. In 2018 alone, 16,000 new vulnerabilities were disclosed. Moreover CVE/NVD misses many vulnerabilities, only accounting for 60% of vulnerabilities tracked by curated databases.

There are two broader categories of threats faced by open source software usage:

- Known Security vulnerabilities (with CVE Published or disclosed by other curated databases)
- New vulnerabilities being introduced into an open source package, but the vulnerability is not yet disclosed.

There are many vendors exist that provide tools to detect and act on published vulnerabilities. We're proposing an open source collaborative project to address the latter: detecting and preventing new vulnerabilities before they impact the industry. This not only improves security of enterprises consuming open source packages, but also empowers open-source developers in detecting and preventing security problems early.

We're proposing a pluggable and extendable infrastructure to security scan all open source packages. This infrastructure allows to add static code analysis tools, binary analysis tools or Fuzzing tools etc.

These tools were used in the past by Security researchers in isolation to hunt for vulnerabilities, malicious files that contain similar known problems. Through this infrastructure, we're able to identify quickly which packages contain malicious files that are like previously known malicious pieces of code. By including these in popular open source repositories and their workflow, package owners are alerted early in lifecycle. This system also allows Security researchers to share their knowledge to the open source community by adding new rules or findings on ongoing basis to this central system.

We're also proposing that open source code repositories should publish security metadata for all hosted open source packages so that data could be programmatically consumed by private, public and government sectors. This would include above proposed Scanning results and other relevant metadata that may impact security posture of underlying package like history of published vulnerabilities, mean time to remediate reported security bugs, frequency of commits etc.