Vulnerable Dependencies in Open-Source Software: the Myth of the Latest Version

by Henrik Plate, Ivan Pashchenko, Serena E. Ponta, Antonino Sabetta, and Fabio Massacci

Abstract

The use of free open-source software (FOSS) components with known vulnerabilities represents a serious threat to %the free open-source software (FOSS) ecosystem, the software industry, given the widespread use of FOSS.

The solution to this problem is supposedly simple: to replace outdated dependencies with the most recent version available. This solution, when applicable, takes for granted that the latest release of a FOSS library does not include, in turn, libraries that are known to be vulnerable.

Our hands-on experience with the analysis of vulnerabilities of Java FOSS components suggested that this assumption does not always hold. This motivated our study to assess systematically whether the latest released versions of open-source projects are indeed free from dependencies with known vulnerabilities.

To conduct our study we built a tool that leverages the functionality of Apache Maven to determine the set of dependencies of a project and then links such information with the detailed content of a vulnerability database that SAP constructed over the past four years as part of its internal FOSS vulnerability management process.

We used our tool to analyze the dependencies of the latest versions of 94 popular FOSS Java projects from GitHub.

Our study shows that (despite considering the latest version) 61% of the projects we analyzed include at least one dependency that is affected by a known vulnerability, and more than a half of these vulnerable dependencies are direct.