Warning: The number of vulnerabilities in open source software are increasing rapidly

Besides malware, spam emails or DDos attacks, vulnerabilities in open source software are also considered as one of the most significant security threats at the moment.

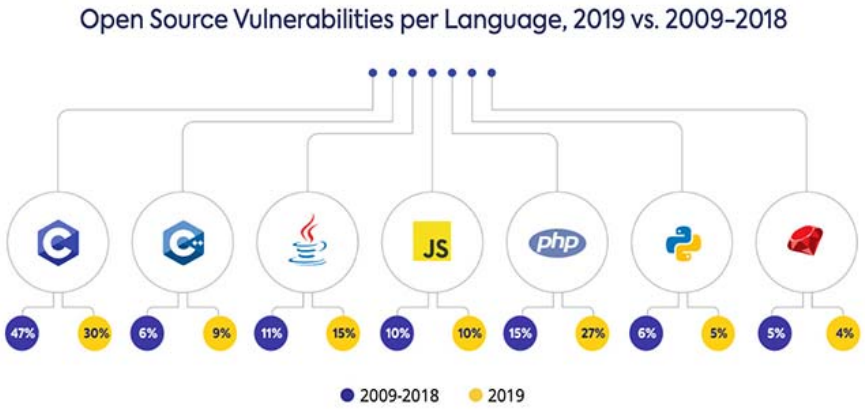
Besides malware, spam emails or DDos attacks, vulnerabilities in open source software are also considered as one of the most significant security threats at the moment.

According to research by cyber security organization WhiteSource, the number of open source software vulnerabilities recorded in 2019 has increased by 50% compared to 2018, from more than 4,000 to more than 6000. However, it is only ' floating iceberg 'because, according to experts, there are still many holes in other open source systems that are silently damaging but not yet discovered or reported.

However, this situation does not surprise many people, even it was foreseen due to the widespread development, massively and somewhat 'out of control' of the open source community in the past few years, together with that being the media attention towards recent data breaches.

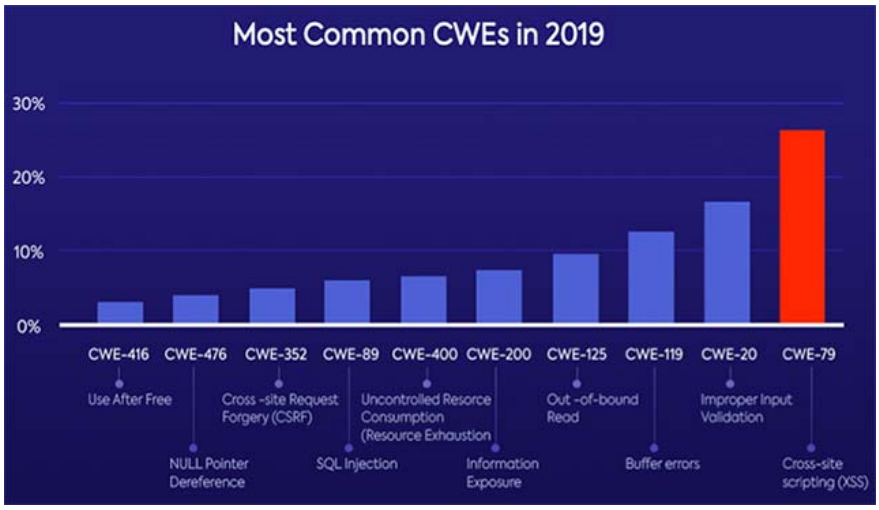
WhiteSource has surveyed more than 650 developers, collected data from the US National Vulnerability Database (NVD), security advisory processes, vulnerability databases as well as many other data sources and found that:

1. More than 85% of open source security vulnerabilities were disclosed with an existing bug fix.
2. Only 84% of the reported open source vulnerabilities are stored in the NVD database, some of which are revealed elsewhere, after a few months.
3. The C programming language still has the highest vulnerability rate (30%) because the amount of code written in this language is quite large. Followed by PHP (27%) and Java (15%).



Noting, Python's increasing popularity is almost proportional to the number of vulnerabilities associated with open source software written in this language. Though to be fair, vulnerabilities are a common result of less secure encryption and many other factors.

Common security vulnerabilities (CWEs) in 2019 included cross-site scripting (XSS), ranked first, followed by input validation vulnerabilities and buffer errors. ranked third, as follows:



Overall, the list of the top 5 most common vulnerabilities for 2019 is not much different from 2018. In 2018, the buffer error ranked second in the list and the third wrong input validation error, in When the remaining positions are unchanged.

According to security experts, most of these vulnerabilities stem from relatively simple flaws in the codebase as well as inaccurate programming problems - elements that can be avoided by Comply with fairly basic coding standards.