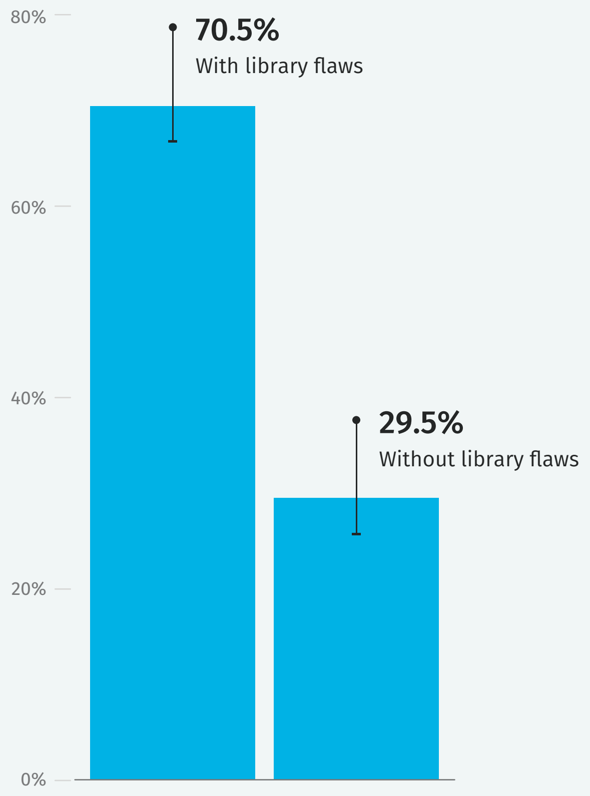
VERACODE

STATE OF SOFTWARE SECURITY
Open Source Edition

For our *State of Software Security: Open Source Edition* report, we analyzed the security of the open source libraries found in 85,000 applications. Below are highlights of that analysis.



Most applications contain vulnerable open source libraries

PERCENT OF APPLICATIONS ON FIRST SCAN:

- With a security flaw in an open source library ***70.5%***
- Without a security flaw in an open source library ***29.5%***

Including any PHP library has a greater than 50% chance of bringing a security flaw with it.

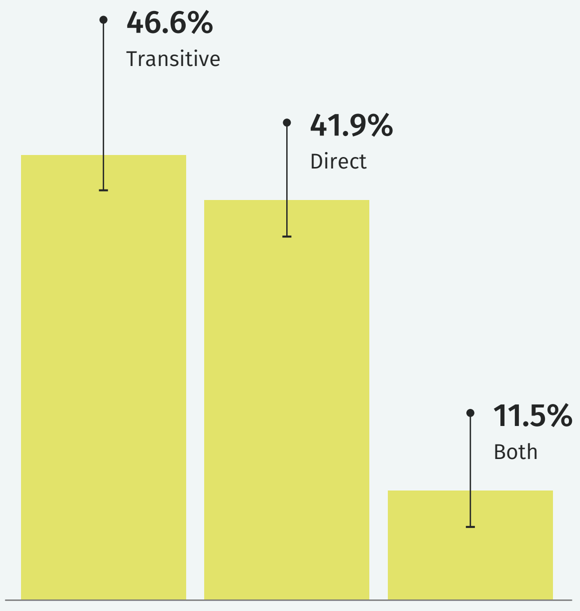
MOST COMMON VULNERABILITIES FOUND IN OPEN SOURCE LIBRARIES:

- Cross-Site Scripting ***30%***
- Insecure deserialization ***23.5%***
- Broken access control ***20.3%***

Most flawed libraries end up in code indirectly

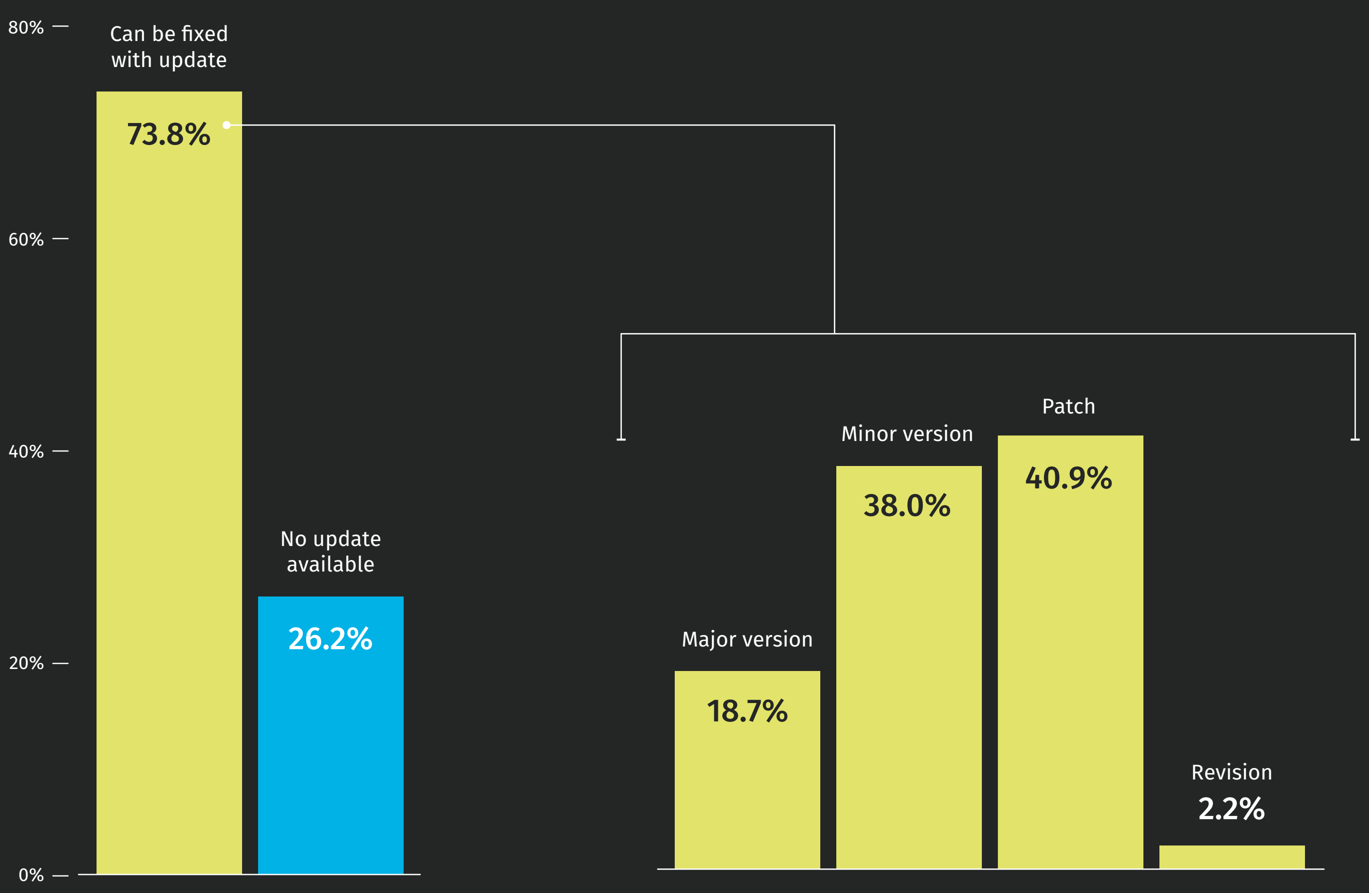
AMONG THE SECURITY FLAWS IN OPEN SOURCE LIBRARIES FOUND IN APPLICATIONS ON FIRST SCAN:

- ***46.6%*** transitive [not pulled in directly by developers, but by another library in use]
- ***41.9%*** direct
- ***11.5%*** both



Fixing not necessarily a major undertaking

Fixing most library-introduced flaws in applications can be accomplished with only a minor version update:



AMONG SECURITY FLAWS FOUND IN OPEN SOURCE LIBRARIES:

- Can be fixed with update ***73.8%***
- No update available ***26.2%***

UPDATE TYPE AVAILABLE AMONG SECURITY FLAWS FOUND IN OPEN SOURCE LIBRARIES:

- Major version ***18.7%***
- Minor version ***38.0%***
- Patch ***40.9%***
- Revision ***2.2%***

Bottom line

There are fixes for these issues, and most are minor – suggesting that this problem is one of discovery and tracking, not huge refactoring of code.

GET THE FULL REPORT