Mid-Year Open Source License Compliance and Vulnerability Check-in

8 Need-to-Know Facts

2021 has been an eventful year for cybersecurity, open source use, and software supply chain management; from increased regulatory requirements such as the U.S. Federal Government's executive order to some fairly high profile cybersecurity attacks and a continued reliance on the development of applications using open source technologies.

The push to develop applications faster while managing the software supply chain and associated risk continues.

Revenera is taking a mid-year look at critical license management and vulnerability data points to help software developers, security experts, and legal professionals better understand the software ecosystems they're part of.

1.800.809.5659 | +44.870.871.1111 | revenera.com

The Facts*

9%

9 percent of issues were disclosed prior to audit start.

1

The number of issues identified for every 17,267 lines of code (over 1.2 billion lines of code scanned).

2,125

The number of issues identified per audit project.

33%

Already in 2021, there's a **33 percent** increase in the number of vulnerabilities found by Revenera audit services.

5.42%

5.42 percent of the vulnerabilities had a high severity rating.

63%

63 percent of the codebases in audit were made up of open source software.

94

P1 issues are the highest priority and should be mitigated expediently. Revenera found **94** issues per project were rated P1.

8.1%

Copyleft licenses include a reciprocity obligation. Commercial organizations sometimes steer away from open source with copyleft licenses because of potential intellectual property issues. **8.1 percent** of the scanned codebase was made up of open source with copyleft licenses.

**Based on Revenera's Audit Services review of six months of data from Software Composition Analysis projects in 2021.*

Key Takeaways

- Open source use continues to increase, however software development teams continue to battle the dynamic nature of both security and license compliance risk. A vulnerability-free library today may look very different tomorrow.
- Access to the right tools, people and processes to detect and remediate open source issues is critical to stopping risk and not spreading it to users and customers.
- Open source licenses include obligations the user must follow in return for using the software. It's critical for security, development, and legal teams to know where open source is being used, the associated licenses, and the steps to remain compliant in order to avoid potential litigation.
- To better manage open source and track usage, deliver a Software Bill of Materials (SBoM) that inventories all open source use including what's found in sub-components, dependencies, and associated licenses. A complete, accurate SBoM enables you to modify open source policies as needed and quickly react to published vulnerabilities.
- The responsibility of open source license and vulnerability management doesn't just fall to one organization. Security, development, and legal teams all have a stake in creating the policies that govern how and where open source is used.
- Software Composition Analysis solutions that scan, detect, and help remediate security and license compliance issues, as well as produce a SBoM, are becoming increasingly important to identify and mitigate open source software risk.

Interested in 2020 license compliance data?

See the full report here.