SYNOPSYS®

Six Findings from the 2024 OSSRA Report That Every Cybersecurity Professional Needs to Know

The 2024 “Open Source Security and Risk Analysis” (OSSRA) report provides insights into the state of open source security, compliance, licensing, and code quality risks in commercial software. Here are six key takeaways from the report.

Finding 1

Open Source Is Everywhere

Ninety-six percent of the 1,000+ codebases examined contained open source. Seventy-seven percent of that code was open source.

96%

of the total codebases **contained** open source

77%

of all code in the total codebases **originated** from open source

Finding 2

With an Average of 562 Open Source Components per App, Manual Testing Can’t Work

At the scale that open source is being used, only automated security testing is feasible.

Finding 3

There Was a 54% Increase in High-Risk Vulnerabilities from 2023

Eighty-four percent of the codebases contained at least one high-risk open source vulnerability.

84%

of codebases assessed for risk contained **vulnerabilities**

Finding 4

Eight of the Top 10 Vulnerabilities Can Be Traced Back to One CWE

A common and dangerous exploit, cross-site scripting, is associated with the majority of the top 10 vulnerabilities highlighted in the OSSRA report.

Finding 5

The Top License Conflict Is Caused by a License Specifically “Not Recommended” for Software

Creative Commons licenses were the most prevalent cause of license conflict, even though Creative Commons, “...recommends against using Creative Commons licenses for software.”

33%

of licenses were **Creative Commons Attribution ShareAlike Licenses**

Finding 6

Open Source Consumers Need to Get Better at Keeping Code Up-to-Date

Ninety-one percent of 900+ risk-assessed codebases contained components 10 versions or more behind the most current version. A third of the codebases were using a version of jQuery vulnerable to the #2 top vulnerability, even though a patch was released in 2020.

91%

of the codebases contained components that were **10 versions** or more behind

There’s much more in the 2024 report to learn, including how to prevent vulnerabilities from entering the software supply chain, ways to protect against risks introduced by AI, and why a Software Bill of Materials can make all the difference in keeping your code secure and license compliant.

Download your copy today