Black Duck Newsroom

New Black Duck Report: 86% of Commercial Codebases Contain Vulnerable Open Source, Exposing Organizations to Security Risks

81% of codebases audited contained high- or critical-risk vulnerabilities, highlighting that blind spots are prevalent when it comes to open source dependency management.

BURLINGTON, Mass., Feb. 25, 2025 /PRNewswire/ -- Black Duck® Software, Inc. ("Black Duck"), a leading provider of application security solutions, today released the tenth annual "Open Source Security and Risk Analysis" (OSSRA) report. The research provides security, development and legal teams with a comprehensive view of the open source landscape, including trends in the adoption and use of open source software, the prevalence of security vulnerabilities and software licensing and code quality risks.

The 2025 OSSRA report is based on the Black Duck Audit team's evaluation of the anonymized findings from 1,658 analyses of 965 commercial codebases across 16 industries during 2024.

This year's report found that 86% of commercial codebases evaluated contained open source software vulnerabilities and 81% contained high- or critical-risk vulnerabilities. Black Duck's data shows that the number of open source files in an average application has tripled, from more than 5,300 in 2020 to more than 16,000 in 2024.

"The 2025 OSSRA report underscores a critical and ongoing challenge for organizations: managing the security and compliance risks inherent in open source software," said Jason Schmitt, CEO of Black Duck. "As open source adoption continues to grow at an incredible velocity, businesses need to implement robust software composition analysis and risk management strategies to build trust into their applications, data and intellectual property."

Additional key findings from the 2025 OSSRA report include:

- **90% of audited codebases were found to have open source components more than four years out-of-date:** Outdated components magnify security risks, provide attackers with an expanded attack surface and create compliance and compatibility issues. The presence of older open source also suggests that developers need to take advantage of software improvements.
- **jQuery was found to be the most frequent source of vulnerabilities:** Eight of the top ten high-risk vulnerabilities were found in jQuery, a widely used JavaScript library. In fact, 43% of the applications Black Duck scanned contained some version of jQuery, frequently an outdated version. The most frequently found high-risk vulnerability was CVE-2020-11023, an XSS vulnerability affecting outdated versions of jQuery, but still present in a third of scanned codebases.
- **56% of the audited codebases contain license conflicts:** Transitive dependencies – open source libraries that other software components rely on to function – caused nearly 30% of the license conflicts found in the audits. Additionally, 33% of codebases contained open source with no license or a customized license.
- **Only 77% of dependencies could be identified via package manager scanning,** suggesting that the remainder were introduced to applications by other means, including AI coding assistants. These blind spots are what lead to lingering unpatched vulnerabilities, outdated components, and license conflicts.

To learn more, download the 2025 OSSRA report, read the blog post, or register for the upcoming March 27 webinar.

About Black Duck

Black Duck®, formerly known as the Synopsys Software Integrity Group, offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Editorial Contact: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

---

https://news.blackduck.com/2025-02-25-New-Black-Duck-Report-86-of-Commercial-Codebases-Contain-Vulnerable-Open-Source,-Exposing-Organizations-to-Security-Risks