Black Duck Newsroom

Synopsys Study Underscores Need for Comprehensive SBOM as Best Defense in Software Supply Chain Security

84% of codebases contained at least one known open source vulnerability, an almost 4% increase from last year's findings

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., Feb. 22, 2023 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the eighth edition of the Open Source Security and Risk Analysis (OSSRA) report. Produced by the Synopsys Cybersecurity Research Center (CyRC), the 2023 OSSRA report examines the results of more than 1,700 audits of commercial and proprietary codebases involved in merger and acquisition transactions and highlights trends in open source usage across 17 industries.

The findings of the 2023 OSSRA report deliver an in-depth look at the current state of open source security, compliance, licensing, and code quality risks in commercial software with the goal of helping security, legal, risk, and development teams better understand the open source security and license risk landscape. This year's findings revealed an overwhelming majority of codebases (84%) contain at least one known open source vulnerability, a nearly 4% increase from last year.

The first step toward reducing business risk from open source, proprietary, and commercial code involves a comprehensive inventory of all software a business uses, regardless of where it comes from or how it's acquired. Only with this complete inventory – a Software Bill of Materials (SBOM) – can organizations establish a strategy to address risk stemming from new security disclosures like Log4Shell.

"The 2023 OSSRA report findings underscore the reality of open source as the underlying foundation of most types of software built today," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "An increase in the average number of open source components rising 13% (from 528 to 595) in this year's audits further reinforces the importance of implementing a comprehensive SBOM that lists all open source components in your applications as well as their licenses, versions, and patch status. This is a foundational strategy towards understanding and reducing business risk by defending against software supply chain attacks."

Key findings from the 2023 OSSRA report include:

- **A five-year overview of OSSRA data shows dramatic growth in open source use**: The global pandemic contributed to the EdTech sector's adoption of open source, which grew by 163%, with educational courses and instructor/student interactions increasingly pushed online. Other sectors experiencing a large spike in open source growth include the Aerospace, Aviation, Automotive, Transportation and Logistics sector with a 97% increase and 74% growth in Manufacturing and Robotics.

- **High-risk vulnerabilities over the past five years have also increased at an alarming rate:** Since 2019, high-risk vulnerabilities in the Retail and eCommerce sector jumped by 557%. Comparatively, the Internet of

Things (IoT) sector, with 89% of the total code being open source, saw a 130% increase in high-risk vulnerabilities in the same period. Similarly, the Aerospace, Aviation, Automotive, Transportation and Logistics vertical was found to have a 232% increase in high-risk vulnerabilities.

- **Use of open source components with no licenses puts organizations at greater risk of violating copyright law than those using licensed components:** The report found that 31% of codebases are using open source with no discernable license or with customized licenses. This is a 55% increase from last year's OSSRA report. The lack of a license associated with open source code, or a variant of another open source license, may place undesirable requirements on the licensee and will often require legal evaluation for possible IP issues or other legal implications.

- **Available code quality and security patches are not applied to a majority of codebases**: Of the 1,480 audited codebases that included risk assessments, 91% contained outdated versions of open source components. Unless an organization keeps an accurate and up to date SBOM, an outdated component can be forgotten until it becomes vulnerable to a high-risk exploit.

"The key to managing open source risk at the speed of modern development is maintaining complete visibility of application contents," said Mike McGuire, senior software solutions manager within the Synopsys Software Integrity Group. "By building this visibility into the application lifecycle, businesses can arm themselves with the information needed to make informed, timely decisions regarding risk resolution. Organizations leveraging any type of third-party software should rightfully assume that it contains open source. Verifying this, and staying on top of the associated risk, is as simple as obtaining an SBOM – something easily provided by a vendor taking the necessary steps to secure their software supply chain."

To learn more about the 2023 OSSRA findings, download a copy of the report, read the blog post, or register for the March 23rd webinar.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software. Learn more at www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As an S&P 500 company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and offers the industry's broadest portfolio of application security testing tools and services. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing more secure, high-quality code, Synopsys has the solutions needed to deliver innovative products. Learn more at www.synopsys.com.

Editorial Contact:

Liz Samet
Synopsys, Inc.
336-414-6753
esamet@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2023-02-22-Synopsys-Study-Underscores-Need-for-Comprehensive-SBOM-as-Best-Defense-in-Software-Supply-Chain-Security