New Synopsys Report Finds 74% of Codebases Contained High-Risk Open Source Vulnerabilities, Surging 54% Since Last Year

The Computer Hardware and Semiconductors industry contained the most open source vulnerabilities classified as high risk, followed by Manufacturing, Industrials and Robotics

SUNNYVALE, Calif., Feb. 27, 2024 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the ninth edition of the annual "Open Source Security and Risk Analysis" (OSSRA) report. The research highlights that nearly three-quarters of commercial codebases assessed for risk contain open source components impacted by high-risk vulnerabilities, representing a sharp uptick from the previous year.

In the 2024 OSSRA report, the Synopsys Cybersecurity Research Center (CyRC) analyzes anonymized findings from more than 1,000 commercial codebase audits across 17 industries. The report 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 as well as the prevalence of security vulnerabilities, and software licensing and code quality risks.

While codebases containing at least one open source vulnerability remained consistent year over year at 84%, significantly more codebases contained high-risk vulnerabilities in 2023. This can potentially be attributed to variables like economic instability and the consequent layoffs of tech workers, reducing the number of resources available to patch vulnerabilities. According to the data, the percentage of codebases with high-risk open source vulnerabilities — those that have been actively exploited, have documented proof-of-concept exploits or are classified as remote code execution vulnerabilities — increased from 48% in 2022 to 74% in 2023.

"This year's OSSRA report indicates an alarming rise in high-risk open source vulnerabilities across a variety of critical industries, leaving them at risk for exploitation by cybercriminals," said Jason Schmitt, general manager, Synopsys Software Integrity Group. "The increasing pressure on software teams to move faster and do more with less in 2023 has likely contributed to this sharp rise in open source vulnerabilities. Malicious actors have taken note of this attack vector, so maintaining proper software hygiene by identifying, tracking and managing open source effectively is a key element to strengthening the security of the software supply chain."

Additional key findings from the 2024 OSSRA report include

- **A "zombie code" apocalypse:** Organizations are depending on outdated or inactive open source components. Ninety-one percent of codebases contained components that were 10 or more versions out-of-date, and nearly half (49%) of codebases contained components that had no development activity within the past two years. The report also found that the mean age of open source vulnerabilities in the codebases was over 2.5 years old, and nearly a quarter of codebases contained vulnerabilities more than 10 years old.
- **High-risk open source vulnerabilities permeate across critical industries** The Computer Hardware and Semiconductors industry had the highest percentage of codebases with high-risk open source vulnerabilities (88%), followed closely by Manufacturing, Industrials and Robotics at 87%. Closer to the middle of the pack, the Big Data, AI, BI and Machine Learning industry had 66% of its codebases impacted by high-risk vulnerabilities. At the bottom of the list, the Aerospace, Aviation, Automotive, Transportation and Logistics industry still had high-risk vulnerabilities in a third (33%) of its codebases.
- **Open source license challenges remain:** License compliance is an important aspect of effective software supply chain management, but the report found that over half (53%) of the codebases contained open source license conflicts, and 31% of codebases were using code with either no discernible license or a customized license. Once again, the Computer Hardware and Semiconductors industry ranked highest in percentage of codebases containing license conflicts at 92% followed by Manufacturing, Industrials and Robotics at 81%. Just one noncompliant license in software can result in loss of lucrative intellectual property, time-consuming remediation and delays in getting products to market.
- **Eight of the top 10 vulnerabilities trace back to one common weakness type** The majority of the open source vulnerabilities that were observed most frequently in this research are classified as Improper Neutralization weaknesses (CWE-707). This weakness type includes the various forms of cross-site scripting that, if exploited, can be quite severe.

To learn more about the 2024 OSSRA findings, download a copy of the report, read the blog post or register for the March 28th 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
Catalyzing the era of pervasive intelligence,Synopsys, Inc. (Nasdaq: SNPS) delivers trusted and comprehensive silicon to systems design solutions, from electronic design automation to silicon IP and system verification and validation. We partner closely with semiconductor and systems customers across a wide range of industries to maximize their R&D capability and productivity, powering innovation today that ignites the ingenuity of tomorrow. Learn more at www.synopsys.com.

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

SOURCE Synopsys, Inc.