Black Duck Newsroom

Software Vulnerabilities Are on the Decline, According to New Synopsys Research

The 2023 Software Vulnerability Snapshot Report Reveals a 14% Decrease in Vulnerabilities Found Over the Past Two Years

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

SUNNYVALE, Calif., Nov. 14, 2023 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today published the 2023 Software Vulnerability Snapshot report. According to the data, analyzed by Synopsys Cybersecurity Research Center (CyRC), there has been a significant decrease in vulnerabilities found in target applications – from 97% in 2020 to 83% in 2022 – an encouraging sign that code reviews, automated testing and continuous integration are helping to reduce common programming errors.

The report details three years of data (2020 - 2022) derived from tests run by Synopsys Security Testing Services, with targets made up of web applications, mobile applications, network systems and source code. Tests are designed to probe running applications as a real-world attacker would, incorporating multiple security testing techniques including penetration (pen) testing, dynamic application security testing (DAST), mobile application security testing (MAST) and network security testing.

Although this is a positive development for the industry, the data also demonstrates that relying on a single security testing solution such as static application security testing (SAST) is no longer sufficient as an approach. For example, server misconfigurations represented an average of 18% of the total vulnerabilities found in the three years of tests. Without a multilayered security approach that combines SAST to identify coding flaws, DAST to examine running applications, SCA to identify vulnerabilities introduced by third-party components, and penetration testing to identify issues that might have been missed by internal testing, these types of vulnerabilities will likely go unchecked.

"For the first time in years, we're seeing a decrease in the number of known vulnerabilities in software, which provides new hope that organizations are taking security seriously and prioritizing a strategic and holistic approach to software security in order to make a lasting impact," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "As hackers have become more sophisticated, a multilayered security approach is needed more than ever to identify where software risks live and protect businesses from being exploited."

Additional findings include

- **High-severity vulnerabilities are less likely**: On average over the past three years, 92% of the tests uncovered some form of vulnerability. However, only 27% of those tests contained high-severity vulnerabilities, and 6.2% contained critical-severity vulnerabilities.
- **Leaked information continues to be a top risk:** The top security issue that was uncovered has remained unchanged from 2020 to 2022 – information leakage, a major security issue occurring when sensitive

information is exposed to unauthorized parties. An average of 19% of the total vulnerabilities were directly related to information leakage issues.

- **Cross-site scripting is on the rise:** Of all high-risk vulnerabilities found in 2022, 19% were found to be susceptible to cross-site scripting attacks.
- **Third-party software poses increased risks:** Among the top 10 security issues in 2022, 25% of the tests conducted found vulnerable third-party libraries to be a risk. Software is likely vulnerable if you do not know the versions of all components in use, including third-party and open source components.

To learn more, download the 2023 Software Vulnerability Snapshot: A Three-Year Analysis of the 10 Most Common Web and Software Application Vulnerabilities or read the detailed blog post.

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/2023-11-14-Software-Vulnerabilities-Are-on-the-Decline,-According-to-New-Synopsys-Research