Synopsys Research Finds Vulnerabilities in 95% of Applications, 25% Impacted by Critical- or High-Risk Vulnerabilities

This year's Software Vulnerability Snapshot report examines prevalence of vulnerabilities identified by Synopsys Application Security Testing Services and Synopsys Cybersecurity Research Center

MOUNTAIN VIEW, Calif., Nov. 15, 2022 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today published the "Software Vulnerability Snapshot: The 10 Most Common Web Application Vulnerabilities." The report examines the results of 4,300 security tests conducted on 2,700 software targets, including web applications, mobile applications, source code files, and networks systems (i.e., software or systems). The majority of the security tests were intrusive "black box" or "gray box" tests, including penetration testing, dynamic application security testing (DAST), and mobile application security testing (MAST), designed to probe running applications as a real-world attacker would.

Eighty-two percent of the test targets were web applications or systems, 13% were mobile applications, and the remainder were either source code or network systems/applications. Industries represented in the tests included software and internet, financial services, business services, manufacturing, consumer services, and healthcare.

In the 4,300 tests conducted, 95% of the targets were found to have some form of vulnerability (a 2% decrease from last year's findings). Twenty percent of the targets had high-risk vulnerabilities (a 10% decrease from last year), and 4.5% had critical vulnerabilities (a 1.5% decrease from last year).

The results demonstrate that the best approach to security testing is to utilize the wide spectrum of tools available including static analysis, dynamic analysis, and software composition analysis to help ensure an application or system is free from vulnerabilities. For example, 22% of the total test targets had some exposure to a cross-site scripting (XSS) vulnerability, one of the most prevalent and destructive high-/critical-risk vulnerabilities impacting web applications. Many XSS vulnerabilities occur when the application is running. The good news is that the exposure identified in this year's findings were 6% lower than last year's findings—meaning that organizations are taking proactive measures to mitigate XSS vulnerabilities in their production applications.

"This research underscores that intrusive black box testing techniques like DAST and pen testing are particularly effective for surfacing exploitable vulnerabilities in the software development lifecycle and should be part of any well-rounded application security testing regimen," said Girish Janardhanudu, vice president, security consulting at Synopsys Software Integrity Group.

Additional report highlights

- **OWASP Top 10 vulnerabilities were discovered in 77% of the targets** . Application and server misconfigurations were 18% of the overall vulnerabilities found in the tests (a 3% decrease from last year's findings), represented by the OWASP A05:2021 – Security Misconfiguration category. And 18% of the total vulnerabilities found were related to the OWASP A01:2021 – Broken Access Control category (a 1% decrease from last year).
- **The urgent need for a software Bill of Materials** . Vulnerable third-party libraries were found in 21%

of the penetration tests conducted (an increase of 3% over last year's findings). This corresponds with the 2021 OWASP Top 10 category A06:2021—Use of Vulnerable and Outdated Components. Most organizations use a mix of custom-built code, commercial off-the-shelf code, and open source components to create the software they sell or use internally. Often those organizations have informal—or no—inventories detailing exactly what components their software is using, as well as those components' licenses, versions, and patch status. With many companies having hundreds of applications or software systems in use, each themselves likely having hundreds to thousands of different third-party and open source components, an accurate, up-to-date software Bill of Materials is urgently needed to effectively track those components.

- **Lower-risk vulnerabilities can also be exploited to facilitate attacks** . Seventy-two percent of the vulnerabilities discovered in the tests are considered low- or medium-risk. That is, the issues found are not directly exploitable by attackers to gain access to systems or sensitive data. Nonetheless, resurfacing these vulnerabilities isn't an empty exercise, as even lower-risk vulnerabilities can be exploited to facilitate attacks. For example, verbose server banners—found in 49% of the DAST tests and 42% of the pen tests—provide information such as server name, type, and version number that could allow attackers to perform targeted attacks on specific technology stacks.

To learn more, download the "Software Vulnerability Snapshot: The 10 Most Common Web Application Vulnerabilities" or read the 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.