Black Duck Newsroom

Synopsys Research Finds Vulnerabilities in 97% of Applications, 36% Impacted by Critical- or High-Risk Vulnerabilities

2021 Software Vulnerability Snapshot report examines prevalence of vulnerabilities identified by Synopsys Application Security Testing Services.

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

MOUNTAIN VIEW, Calif., Nov. 16, 2021 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today published "2021 Software Vulnerability Snapshot: An Analysis by Synopsys Application Security Testing Services," a report examining data from 3,900 tests conducted on 2,600 targets (i.e., software or systems) during 2020. The data, compiled by tests performed by Synopsys security consultants in our assessment centers for our customers, included penetration testing, dynamic application security testing, and mobile application security analyses, designed to probe running applications as a real-world attacker would.

Eighty-three percent of the tested targets were web applications or systems, 12% 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, media and entertainment, and healthcare.

"Cloud-based deployments, modern technology frameworks, and the rapid pace of delivery is forcing security groups to react more quickly as software is released," said Girish Janardhanudu, vice president, security consulting at Synopsys Software Integrity Group. "With insufficient AppSec resources in the market, organizations are leveraging application testing services such as those Synopsys provides in order to flexibly scale their security testing. We've seen a heavy increase in assessment demand throughout the pandemic."

In the 3,900 tests conducted, 97% of the targets were found to have some form of vulnerability. Thirty percent of the targets had high-risk vulnerabilities, and 6% had critical-risk vulnerabilities. The results demonstrate that the best approach to security testing is to utilize the wide spectrum of tools available to help ensure an application or system is free from vulnerabilities. For example, 28% of the total test targets had some exposure to a cross-site scripting (XSS) attack, one of the most prevalent and destructive high- /critical-risk vulnerabilities impacting web applications. Many XSS vulnerabilities occur only when the application is running.

Other report highlights

- **2021 OWASP Top 10 vulnerabilities were discovered in 76% of the targets.** Application and server misconfigurations were 21% of the overall vulnerabilities found in the tests, represented by the OWASP A05:2021—Security Misconfiguration category. And 19% of the total vulnerabilities found were related to the OWASP A01:2021—Broken Access Control category.

- **Insecure data storage and communication vulnerabilities plague mobile applications.** Eighty percent

of the discovered vulnerabilities in the mobile tests were related to insecure data storage. These vulnerabilities could allow an attacker to gain access to a mobile device either physically (i.e., accessing a stolen device) or through malware. Fifty-three percent of the mobile tests uncovered vulnerabilities associated with insecure communications.

- **Even lower-risk vulnerabilities can be exploited to facilitate attacks.** Sixty-four percent of the vulnerabilities discovered in the tests are considered minimal-, low-, or medium-risk. That is, the issues found are not directly exploitable by attackers to gain access to systems or sensitive data. Nonetheless, surfacing these vulnerabilities is not an empty exercise, as even lower-risk vulnerabilities can be exploited to facilitate attacks. For example, verbose server banners—found in 49% of the tests—provide information such as server name, type, and version number, which could allow attackers to perform targeted attacks on specific technology stacks.

- **An urgent need for a software Bill of Materials.** Of note was the number of vulnerable third-party libraries in use, found in 18% of the penetration tests conducted by Synopsys Application Testing Services. This corresponds with the 2021 OWASP Top 10 category A06:2021—Use of Vulnerable and Outdated Components. Most organizations typically 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.

To learn more, download the "2021 Software Vulnerability Snapshot: An Analysis by Synopsys Application Security Testing Services," or read the blog post.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle. 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.
703-657-4218
esamet@synopsys.com

---

https://news.blackduck.com/2021-11-16-Synopsys-Research-Finds-Vulnerabilities-in-97-of-Applications,-36-Impacted-by-Critical-or-High-Risk-Vulnerabilities