Black Duck Newsroom

Synopsys Research Reveals Significant Security Concerns in Popular Mobile Apps Amid Pandemic

Analysis of 3,335 popular Android apps shows the majority contain security vulnerabilities

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

MOUNTAIN VIEW, Calif., March 25, 2021 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the report, Peril in a Pandemic: The State of Mobile Application Security Testing. The report, produced by the Synopsys Cybersecurity Research Center (CyRC), examines the results of a study of the 3,335 most popular Android mobile apps on the Google Play Store in the first quarter on 2021. The report found the majority of apps (63%) contained open source components with known security vulnerabilities and highlighted other pervasive security concerns including sensitive data exposed in the application code and the use of excessive mobile device permissions.

The research, which was conducted using Synopsys Black Duck Binary Analysis[1], focused on 18 popular mobile app categories, many of which have seen explosive growth during the pandemic, including business, education, and health & fitness. The apps ranked among the most downloaded or top grossing on the Google Play Store. While the security analysis results vary by app category, at least one-third of the apps in all 18 categories contained known security vulnerabilities.

"Like any other software, mobile apps are not immune to security weaknesses and vulnerabilities that can put consumers and businesses at risk," saidJason Schmitt, general manager of the Synopsys Software Integrity Group. "Today, mobile app security is especially important when you consider how the pandemic has forced many of us—including children, students, and large portions of the workforce—to adapt to increasingly mobile-dependent, remote lifestyles. Against the backdrop of these changes, this report underscores the critical need for the mobile app ecosystem to collectively raise the bar for developing and maintaining secure software."

Open source vulnerabilities in mobile apps are pervasive. Out of the 3,335 apps analyzed, 63% contained open source components with at least one known security vulnerability. Vulnerable apps contained an average of 39 vulnerabilities. In total, CyRC identified more than 3,000 unique vulnerabilities, and they appeared more than 82,000 times.

Known vulnerabilities are a solvable problem. While the number of vulnerabilities uncovered in this research is daunting, it is perhaps more surprising that 94% of the vulnerabilities detected have publicly documented fixes, meaning there are security patches or newer, more secure versions of the open source component available. Furthermore, 73% of the vulnerabilities detected were first disclosed to the public more than two years ago, indicating that app developers simply aren't considering the security of the components used to build their apps.

In-depth analysis of high-risk vulnerabilities. A more thorough analysis revealed that nearly half (43%) of the vulnerabilities are considered by CyRC to be high risk because they either have been actively exploited or are associated with documented proof-of-concept (PoC) exploits. Just under five percent of the vulnerabilities are

associated with an exploit or PoC exploit *and* have no fix available. One percent of the vulnerabilities are classified as remote code execution (RCE) vulnerabilities—which is recognized by many as the most severe class of vulnerability. 0.64% are classified as RCE vulnerabilities *and* are associated with an active exploit or PoC exploit.

Information leakage. When developers unintentionally expose sensitive or personal data in the source code or configuration files of an application, it can potentially be used by malicious attackers to mount subsequent attacks. CyRC found tens of thousands of instances of information leakage, where potentially sensitive information was exposed, ranging from private keys and tokens to email and IP addresses.

Excessive use of mobile device permissions. Mobile apps often require access to certain features or data from your mobile device to function effectively. However, some apps recklessly or surreptitiously require far more access than necessary. The mobile apps analyzed by CyRC require an average of 18 device permissions. That includes an average of 4.5 *sensitive* permissions, or those that require the most access to personal data, and an average of 3 permissions that Google classifies as "not intended for third-party use." One app with over 1 million downloads required 11 permissions that Google classifies as "Protection Level: Dangerous." Another app with over 5 million downloads required a total of 56 permissions, 31 of which Google classifies as "Protection Level: Dangerous" or as signature permissions that are not to be used by third-party apps.

Comparing app categories. At least 80% of the apps in six of the 18 categories contained known vulnerabilities, including games, banking, budgeting, and payment apps. The lifestyle and health & fitness categories tied for the lowest percentage of vulnerable apps at 36%. The banking, payment, and budgeting categories also ranked in the top three for highest average number of mobile device permissions required, well above the overall average of 18. Games, tools for teachers, education, and lifestyle apps required the lowest average number of permissions.

To learn more, download the report, Peril in a Pandemic: The State of Mobile Application Security Testing.

1. Black Duck Binary Analysis is a unique feature of the Black Duck software composition analysis offering that can be used to detect security vulnerabilities, information leakage and mobile device permissions in software. Unlike most other software analysis tools, it analyzes compiled binaries instead of source code, meaning it can scan virtually any software, from desktop and mobile applications to embedded system firmware. To learn more, watch the Black Duck Binary Analysis webinar.

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 Contacts:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2021-03-25-Synopsys-Research-Reveals-Significant-Security-Concerns-in-Popular-Mobile-Apps-Amid-Pandemic