Name: Archit Benipal

Subject: Software Supply Chain Security (CY 653)

Assignment: Open-Source Security

Summary for Opensource Security and Risk Analysis Report 2023:

Introduction:

OSSRA as the title suggests produces the state of opensource security, compliance, licensing, and code quality risks in commercial software annually to better understand the opensource security landscape. The 2023 OSSRA report presents data from 2022, analyzing over 1,700 codebases across 17 industries, identifying software risks during M&A transactions. Synopsys' Black Duck SCA and the CyRC Audit Services support security, and compliance programs by identifying and tracking opensource code, thereby managing open source risks effectively. The CyRC includes data on more than 6.1 million opensource components from over 28000 forges and repositories.

Overview:

In year 2022 out of 1703 codebases scanned, 87% included security and operational risks. The percentage being 54 % of codebases with license conflicts, 89% of the codebases contained outdated opensource and 91% with no new development in the past two years. As per the graph high-risk vulnerabilities with working PoC saw its peak in the year 2020.

The 2023 OSSRA report analyzed 1,703 codebases, finding 96% contained open source, which made up 76% of the total code. Each application had an average of 595 opensource components. Due to the volume, automated solutions like SCA are required for managing security vulnerabilities. Alarmingly, 84% of codebases had at least one known vulnerability, a 4% rise from 2022. Additionally, 48% contained high-risk vulnerabilities, only a 2% decrease from the previous year. According to the report it clarifies that “Percentage of codebases containing at least one vulnerability” was always above 60% for the last five years and compare that with high-risk vulnerability which was at peak in 2020, which has decreased since then but is still growing at an alarming rate. The most vulnerable components according to the report is jQuery a JavaScript framework designed to simplify certain tasks in contrast to that the least vulnerable components are php and Linux kernel which are still used to this day but are less prevalent among developers.

A recent report co-sponsored by Synopsys and the Enterprise Strategy Group revealed growing concerns about open source and supply chain security. Seventy-three percent of the surveyed organizations admitted to bolstering their efforts to secure opensource software, container images, and third-party software components due to recent supply chain attacks. Furthermore, 34% experienced exploits that exploited known opensource software vulnerabilities within the last year. In the wake of President

Biden's Executive Order 14028, organizations are still grappling with supply chain fundamentals such as understanding their software supply chain's breadth, ensuring visibility into their dependent software, and meeting increasing transparency demands. The complexity of supply chain security arises from the multitude of elements involved in its creation, affecting both the final product and its users. Therefore, thorough verification of the security of open source and third-party software is paramount in order not to place unwarranted trust in the weakest links of the supply chain. As this Gartner has estimated more than 45% of organizations world-wide will experience software supply chain attacks by 2025. It's clear that the security of opensource software and the broader software supply chain is a growing concern for many organizations. These worries are motivated by the increasing prevalence of opensource code in applications and the escalating number of known vulnerabilities and high-risk exploits associated with opensource components.

The report also reveals opensource code is ubiquitous across all industries, even in those traditionally less reliant on it, with many codebases containing high-risk vulnerabilities. The Synopsys vulnerability severity scoring system, used in their Black Duck Security Advisories (BDSAs), helps assign precise CVSS scores considering various factors, including exploitability and temporal metrics, enabling accurate risk prioritization. Even though the common vulnerabilities are available publicly ,still encounter then in the analyzed codebases. This underscores the pervasive use of opensource code across sectors, often coupled with high-risk vulnerabilities. This points to the urgent need for effective management and patching strategies. Synopsys' tailored vulnerability scoring system, factoring in multiple variables, provides a nuanced tool for addressing these risks accurately and promptly.

Over the past five years, the use of opensource code has grown dramatically across sectors, with notable increases in EdTech (163%), Aerospace and Transportation (97%), and Manufacturing and Robotics (74%). However, this has corresponded with an alarming increase in high-risk vulnerabilities, particularly in the Retail and eCommerce sector (557%). In the IoT sector, 100% of scanned codebases contained open source, accompanied by a 130% rise in high-risk vulnerabilities since 2018. This reveals the need for vigilant management and patching in industries increasingly reliant on opensource software. The two sectors where we saw high-risk vulnerabilities most prevalent are the Retail and commerce and computer hardware and semiconductors as these two sectors face the toughest competition in the market.

The Black Duck Audit Services team reported that 54% of all audited codebases in 2022 contained open source with license conflicts, a slight increase from the previous year, but significantly lower than 2020 (65%). The main cause of conflict was the Creative Commons ShareAlike 3.0 license, with 85% of conflicts involving content from Stack Overflow. While there's been a decrease in license conflicts across industries, 31% of the audited codebases were using code with no discernible or customized license, a risky practice that's increased by 55% from last year, and may result in potential IP issues. The most number of conflicts we can find in “Creative Commons Attribution ShareAlike 3.0” reason being:

i. Broad usage -> Due to its versatility it is often used in various projects, leading to its wide distribution.
ii. Combination with other licenses-> If a project combines a license code CC BY-SA 3.0 with different or incompatible license a conflict can occur.

iii. Stack Overflow or other Q&A sites-> Developers often copy code snippets from answers on Stack Overflow into their projects without realizing that this code carries the CC BY-SA 3.0 license, which can then conflict with the license of the larger project.

Using open source is quite common but without proper maintenance the codebases using them are at risk. Sometimes the DevOps is to lazy or completely unaware of the latest update to the opensource component. The Percentage of codebases with open source more than four years out-of-date is increasing per year, the reason being there is no proper incentive program for the community to update or maintain the open source components or repositories.

Log4Shell vulnerability remains present in many codebases due to organizations' unawareness or difficulty in patching foundational components. The persistence of such vulnerabilities is linked to an inherent trust in open source and failure to identify these components in applications. To mitigate business risks from such vulnerabilities, a comprehensive software inventory is crucial, enabling security teams to create strategic plans for addressing potential security issues.

Conclusion:

Amidst the rise in software supply chain attacks, trusting in software security is insufficient without necessary verification. Organizations need to adopt a 'Trust, but Verify' approach, viewing their security through the lens of business risk. The Software Bill of Materials (SBOM), which provides a comprehensive inventory of all software components, is an essential tool for this purpose. SBOMs provide visibility into the 'ingredients' of applications, ensuring compliance, security, and quality. It allows organizations to move from simply trusting in their security to actively verifying it.