SYNOPSYS®

WHITE PAPER

Secure? The State of Open Source Security in Financial Services.

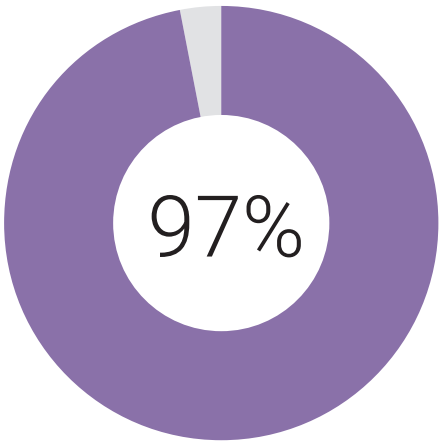
The Synopsys Cybersecurity Research Center's (CyRC) mission is to publish security advisories and research to help organizations better develop and consume secure, high-quality software. Each year, the CyRC performs an in-depth analysis of the current state of open source security, aimed at providing feedback that can be used to inform and guide security-related decisions across industry verticals.

For this year's annual report, the CyRC analyzed over 1,500 codebases across 17 industries. The findings underscore previous iterations of this report and highlight the prevalence of open source libraries across nearly every application in every industry. Central to the popularity of open source, however, is the associated risks it carries when managed improperly or insufficiently.

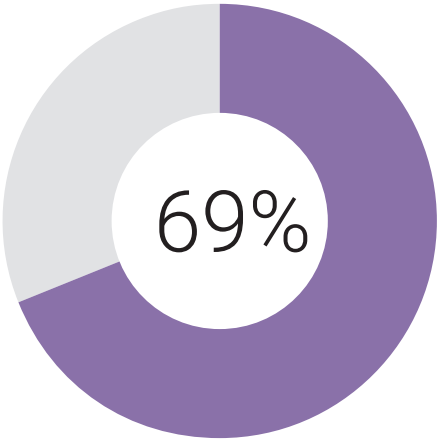
This is particularly true for the applications that fuel the financial services industry (FSI). Entrusted with managing and consuming sensitive data, FSI applications demand a comprehensive approach to application security (AppSec). In an effort to highlight key findings specific to the FSI, we narrowed the focus of the full 2021 "Open Source Security and Risk Analysis" report to create this concentrated piece. It digs into our findings specific to the financial services industry, helping to provide key areas of focus and attention for those tasked with securing FSI applications.

FSI open source vulnerability findings

As the popularity of open source continues to explode, so does its reach across industries. Of the 162 financial services and FinTech applications scanned for this study, 97% contained open source of some kind. Put differently, open source made up 69% of the total codebases in FSI applications.



of the FinTech applications scanned for this study contained open source



of the codebases were comprised of open source

Concerningly, 62% of the total FSI codebases scanned contained open source vulnerabilities. This large number of vulnerabilities denotes an absolute need for open source security considerations and remediation activities specific to the FSI. Of all industries examined, FSI applications were third-highest in total number of vulnerabilities.

Our annual report always notes that a great number of the vulnerabilities we discover are either easily fixable or have had known fixes for long periods of time. This year was no different. All of the top 10 CVEs made an appearance in this year's analysis. CVEs are the vulnerabilities and exposures seen most commonly in publicly released software. They are listed in the CVE database, providing an easily accessible repository for developers. The presence of all 10 of the most prevalent vulnerabilities in our study indicates a failure to remediate simple and well-known vulnerabilities.

The presence of known and unremedied vulnerabilities, in tandem with the sheer number of identified vulnerabilities across FSI apps, points toward a struggle to manage open source. Development teams are falling behind in their efforts to adapt to the dynamic nature of open source security risk. And that is made more troubling by the sensitive nature of FSI data.

Each year, thousands of new open source vulnerabilities are reported. Unlike commercial software, open source has no single vendor to keep users informed of these vulnerabilities or help ensure that security teams have implemented the latest security updates.

Open source is widely used, and open source vulnerabilities and exploits are widely reported—often on the same day they're discovered. This gives hackers the head start they need to compromise thousands of applications and websites. As Heartbleed and the Equifax breach show, a single open source vulnerability can give hackers the keys to thousands of applications.

The moment a vulnerability goes public, organizations are easy targets. It's critical for security teams to find and fix the vulnerable open source in their applications before it can be exploited. Solutions like software composition analysis (SCA) tools help provide a complete view of the open source in use and timely reporting of newly discovered vulnerabilities. The use of open source impacts the overall risk of an organization, so it demands a comprehensive and tactical approach to open source management in order to reduce negative impacts to the business.

Licensing conflict findings

Every year, our analysis highlights the ongoing need for increased attention to the management of open source licenses. Understanding license risk and its impacts to an organization's overall risk posture is critical. Even the friendliest open source licenses include obligations the user takes on in return for use of the software. With open source license litigation on the rise, special attention to licensing concerns is prudent. Organizations must work to track and manage open source with tools and solutions capable of identifying license violations that can result in costly litigation or compromise valuable intellectual property. Our study found that 62% of the scanned FSI codebases contained license conflicts.

While organizations undoubtedly understand that the use of open source entails the need to manage the associated licenses, this report's findings show that few are adequately tackling licensing conflicts. Open source components are governed by a variety of open source licenses, and the details of these licenses are often convoluted. In particular, certain technical and complex licensing conditions can easily pose compliance challenges.

The main challenge caused by open source licensing is that these licenses are subjective. Their interpretation depends on the technical usage of the licensed software. This makes it difficult to determine what legal risks they pose. Compounding this issue, most developers have little to no legal expertise, leaving interpretations up to individuals not equipped to handle such a task.

License management therefore requires a broad classification of licensing based on the risks they pose to legal compliance. Use of SCA tools helps to automate this daunting task, as they can easily identify points of conflict and concern, and help prioritize major license conflicts.

62% of the scanned FSI codebases contained license conflicts

Operational risk findings

Maintaining an active role in sustaining open source often poses an operational burden on organizations' security teams. This year, of the 1,500+ codebases examined by Black Duck® Audit Services, a staggering 91% contained at least one dependency on an open source project that had seen no development activity in the last two years. This means that 91% of codebases received none of the feature upgrades, code improvements, or security fixes they needed for two years.

Of the 162 FSI codebases scanned, 10% had seen zero development activity in the past two years. The same 10% had open source components that were more than four years out-of-date. While 10% is not exceptionally high, it's still concerning that any components have been left untouched for such a long period of time.

Of the 162 FSI codebases scanned, 10% had seen zero development activity in the past two years and had open source components that were more than four years out-of-date.

Open source has increased in popularity in part thanks to the people behind it: the volunteer communities that continuously update code and address vulnerabilities. But the problem with this model is the lack of guarantee; there's no way to be certain that the community has effectively and efficiently kept an open source project up-to-date. Furthermore, there's no way to ensure that those in the community have the skills and resources to adequately maintain the code.

The answer for financial services firms is to implement solutions capable of identifying this code in order to help effectively maintain it. The best way to track the components in your code is to use an SCA tool. Failure to adequately track open source code presents a potential nightmare scenario for security and operations. From a security perspective, the challenge is preventing unpatched vulnerabilities from being exploited. From an operations perspective, the challenge is uncertainty whether your applications are built on or around an open source project that will soon be unusable.

A robust SCA tool helps easily identify out-of-date components and vulnerabilities. It also provides a Bill of Materials to help identify what's in your applications, since you simply can't manage or protect what you don't know you have.

Key takeaways

With open source comes risk, due primarily to organizations lacking tools and practices that help identify the types and quantities of open source in their applications. Failure to grasp a complete picture of the open source across an organization's applications—and its associated licensing obligations and vulnerabilities—puts businesses at significant risk of litigation, exploit, and the possibility of jeopardizing their ownership rights to their software.

The results uncovered by our open source analysis underscores this message and the message we voice each year: open source management continues to be challenging for organizations across all industries.

Every year, we also highlight the availability of security practices and solutions to help easily remedy open source security risks. Redirecting resources and focus within security teams toward adopting a robust open source security program offers security assurances that reliance on open source communities simply cannot provide. The potential threat posed by unidentified licensing conflicts is also easily avoided when the right solutions and practices are prioritized.

Solutions like Synopsys Black Duck SCA help keep development, security, and risk management teams informed of open source vulnerabilities, licensing conflicts, and operational risks. Armed with a tool like Black Duck, teams can take informed actions and streamline application security.

To learn more about Black Duck SCA, visit our website or watch to our recent webinar.

To learn more about our complete findings, read the full "Open Source Security And Risk Analysis" report.

SYNOPSYS®

The Synopsys difference

Synopsys 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.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com