Sencha
An Idera, Inc. Company

3 OPEN SOURCE PROBLEMS KEEPING YOU UP AT NIGHT

AND HOW TO OVERCOME THEM

Kirti Joshi

Introduction

The Open Source model is a radical driver of sustainable development and is popular because of the strong sense of community, collaboration and transparency it instills in its developer base.

Many businesses in this modern era are building their web, mobile and cloud solutions on open source infrastructures. Closed source SaaS companies are joining in the open source effort by offering community versions of their software. There is no doubt that such cohesive efforts are important to seed the ecosystem and encourage collaborative innovation.

What many businesses may not be prepared for is the dark side of open source—when things go wrong overnight, when you least expect them to. In fact, what might be keeping many executives up at night is the constant worry about whether their business data is secure and if their teams have implemented the appropriate safeguarding mechanisms. According to Sonatype's DevSecOps Community Survey[1] of over 5,500 IT professionals, open source security breaches have increased by 71% over the last five years. And 41% of executives do not implement or enforce open source governance in their organizations—a worrisome fact given the prevalence of open source in about 90% of applications.

"Community-based" technology making use of open standards is perceived as the unrivaled choice, but enterprises may not be aware of the significant hidden risks it carries. This short guide highlights the top three open source problems that every team should be aware of.

OPEN SOURCE
SECURITY BREACHES
HAVE INCREASED BY **71%**

3 Open Source Problems to Watch Out For

1. DELAYED SOFTWARE PATCHES

There have been countless security breaches in this recent age of cybercrime. Data breaches, small or large, can cause significant damage to the reputation of the company while presenting unfathomable legal and financial ramifications. With open source adoption, teams have a greater responsibility to ensure that the software used is patched as soon as vulnerabilities are detected. Moreover, the later in the development cycle that a vulnerability is detected, the more expensive it is to remedy. Companies often spend additional money and resources on vulnerability detection tools to speed up this process. But what if there isn't a patch available immediately or you can't anticipate when it will be available? What if the open source developer isn't actively maintaining the code included in your application? In such circumstances, externally facing or mission-critical apps are particularly on the line. Teams could spend weeks analyzing how the vulnerability affects their code in order to find replacement solutions. Or as a last resort, they may even have to temporarily take down their application—causing considerable financial implications. Inevitably, the risks with open source tend to be high, and enterprises are obligated to stay vigilant and address issues promptly.

2. KEEPING YOUR CODE SECURE AND COMPLIANT

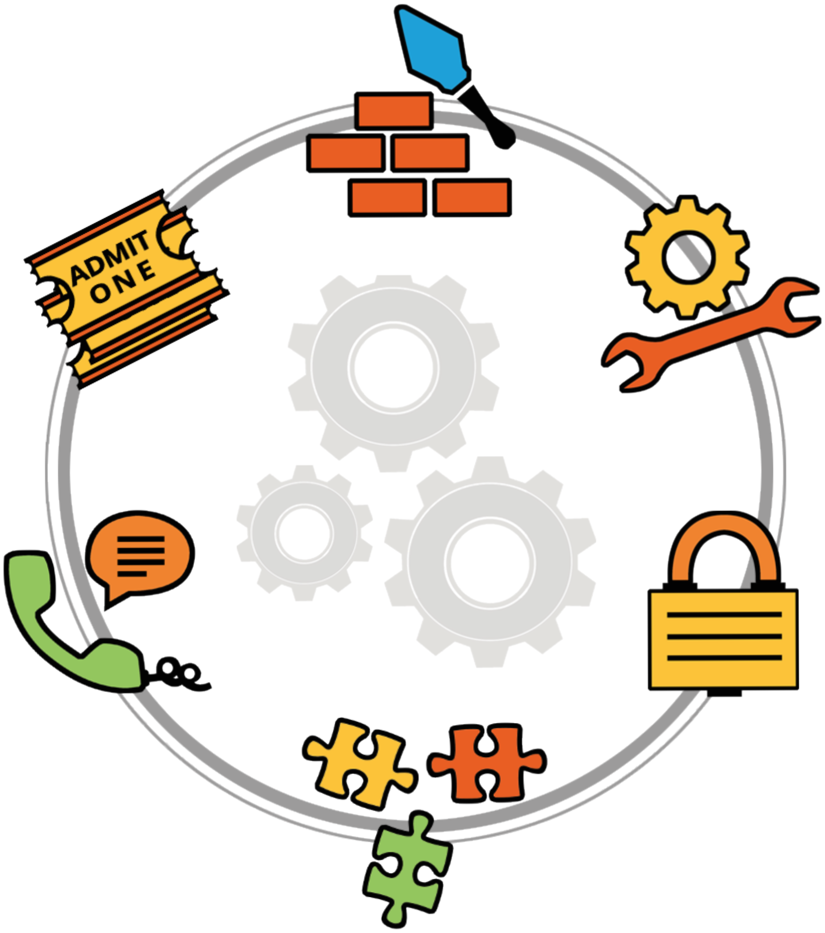
Open source is ubiquitous, and as a result, it is relatively easy for development teams of all sizes to find and incorporate open solutions in their projects. But most teams don't accurately manage and maintain a complete record of open source components used in their products. This can have long-term, severe implications if executives are not enforcing strong software legal compliance (SWLC) policies within their teams. According to a blog[2] published by NPM, "It's common for modern JavaScript projects to depend on 700-1200 packages"! Things can quickly get out of hand if teams are not keeping a close tab of the code sources, their validity and incorporating policies for whitelisting.

3. FAILING TO UNDERSTAND LICENSE NUANCES

Developers need to be extra cautious about the license terms and conditions when selecting open source code to incorporate into projects. Software licenses can be quite complex—some allow redistribution while others don't, and some may work fine standalone but can have subtle nuances and clash with other license types. Things can get tricky, especially where there are gray areas, and consequently, such scenarios always carry some element of risk. It is important that developers using open source code interpret the license terms properly and even take precautionary action by reading between the lines to minimize any foreseeable legal risks. Are you aware of every single license restriction in your application?

Sencha Solutions—Smarter, Safer

Most problems discussed here can be mitigated by adhering to the legal compliance of your codebase and being vigilant regarding the security vulnerabilities that code is exposed to. Oftentimes, situations aren't completely under your control, and the safer choice is to go with an enterprise solution backed by a single entity—where usability, security, and modernization are the whole and sole of their existence. And then there is always someone to reach out to for immediate help.



BUILDING ENTERPRISE-GRADE APPLICATIONS

OPEN SOURCE		SENCHA
Shop, evaluate, configure components. Code enhancements for missing capabilities	**UI Components**	All the components to build stunning apps. 140 components include grids, trees, advanced charting and many more
Develop separately for each platform/browser ensuring design consistency. Steep development and maintenance costs	**Browser/Platform Support**	Develop single “universal” app that works across all platforms, supporting wide range of browsers. No extra maintenance costs
Additional testing overhead. Potential open source security threats	**Testing and Security**	Pre-built, Professionally Tested, High-Performance, Secure UI components
Deficiencies in code maintenance. Potential component interoperability issues	**Interoperability**	Components that interoperate seamlessly with JS framework of choice or no framework at all
Lack of detailed documentation. No dedicated professional support or human to talk to	**Technical Support**	Excellent documentation, examples & technical training. Premium support and expert technical team for guidance
Legal risk associated with restrictive, semi-permissive open source licenses	**Licensing**	Flexible Licensing (single /multi- developer; perpetual or annual)

Minimize your teams' legal risk and maximize productivity by choosing professionally built, high performing components and tools that interoperate with each other. With Sencha products, you don't have to stress about the next vulnerability threat, worry about license incompatibilities, or maintain an exhaustive list of code sources and component whitelisting. Instead, you get back valuable time and resources so that you can augment your applications with modern features that drive business growth. Don't let these worries keep you up at night—make the smarter, safer choice for your team.

EXPLORE SENCHA SOLUTIONS

SOURCES:

[1] Sonatype, "DevSecOps Community Survey" 2019

[2] The npm Blog "Why use SemVer" 22 June, 2017

HELPFUL LINKS: View Examples Resource Center Read the Getting Started Guides

Sencha
An Idera, Inc. Company