Defending Federal Interests: Open Source Security

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Tidelift, December 2023.

The Advanced Technology Academic Research Center (ATARC) and Tidelift brought together government and industry leaders to discuss the challenges and approaches to open source security. Roundtable participants shared their insights and experiences on the open source landscape, the myriad challenges with securing such a dynamic environment, and ways to improve open source security for government agencies.

The Open Source Landscape

> **"Open source is in everything. Whether you're using it directly or if it's baked into something, it's there."**

Agencies are approaching open source security from several angles, all of which intertwine to create a complex ecosystem that's challenging to manage. Open source code is in most, if not all, software products used by government agencies. Open source has become the modern application development platform, and government agencies are using it because it is a vast resource of freely available code that allows agencies to get more work done more quickly, and thus make better use of taxpayer dollars. By building with open source code vs. writing new code from scratch, the government can take advantage of the best and most innovative technology available. The cost of being able to access that stream of constant innovation is that open source is not typically supported by commercial vendors, but is often written by volunteers who have neither the time nor incentives to ensure the software they wrote meets the standards that government agencies would expect from code they write themselves. This leads to security and maintenance issues that stem from unmaintained or undermaintained code. Even one line of compromised code will open an agency up to vulnerability.

The challenge becomes locating vulnerabilities buried layers deep within a piece of software. Panelists note that scanning open source software for vulnerabilities is often not effective. Manual testing can find many of these issues, but to ensure the entire open source library is free of vulnerabilities would require inspecting millions of lines of code. While it may not be easy for government agencies to locate vulnerabilities within open source libraries, the malicious code is still available to an adversary.

Static assessments, such as using a static scanner, are useful to detect known vulnerabilities before running software. This is especially important for developers as they add capabilities or revise software. Implementing a more dynamic assessment allows agencies to consider broader security implications, such as whether the software passes API keys securely or what aspects of the software are visible to adversaries from a black box perspective.

Ultimately, agencies need to automate as many of these processes as possible. Panelists emphasize the need for methodologies and processes to successfully and safely incorporate open source components into the enterprise. Panelists note that nearly 1 in 10 open source components have known vulnerabilities, and there has been a 71% increase in confirmed open source related breaches since 2014. These statistics reinforce the importances of having the correct business practices in place to identify vulnerabilities upfront.

Challenges with Open Source Security

Panelists routinely referenced Zero Trust methodology when discussing open source security. The same concepts apply to vetting and trusting open source data, but the process is not as straightforward in practice. The vastness of open source data libraries combined with the layering effect of open source data within software make it extremely challenging to validate and identify vulnerabilities quickly enough to make a difference.

By nature, open source software is continuously updating, changing, and introducing potential risk. Keeping up with the pace of change requires near constant software patching, which is an unsustainable practice for developers. A patch issued yesterday may be irrelevant tomorrow.

While many agencies have processes in place to implement patches and updates, the process for patching open source software is less clear. In many instances, patches issued do not reach down to the software level.

> **"There's so much room for this to be painful."**

The legal and licensing component of open source data is becoming an additional challenge for many agencies. As the government continues to drive innovation with open source data, the legal components are becoming difficult to track and manage, opening agencies up to liability.

Panelists also note that continuously modifying contracts to ensure a vendor's capabilities is not an agile or simple process. To avoid having to continuously modify vendor contracts, agencies are working to establish agile processes that trust and verify the vendor's open source security protocols, such as using a shift left practice.

Not knowing the origin of open source code is the heart of the problem for government. To attenuate this, some vendors, including Tidelift, are entering into contractual agreements with the open source community, whereby open source developers are paid and sign tax documentation. This allows vendors to know who their open sources are and to ensure their projects meet standards like the NIST Secure Software Development Framework.

Panelists agree agencies need to be doing more to enhance open source security. One panelist recommends agencies should vet application libraries before releasing them to the developer. Another panelist noted that many agencies are not able to access or research CVSS scores lower than 7 or 8, but there are plenty of vulnerabilities contained in lower CVSS scores that must be analyzed.

Agencies should also be aware of the transitive dependencies of open source coding. Understanding how different open source capabilities interact and identifying areas where an adversary can potentially leverage to breach an enterprise is critical. The expanding attack surface offers more opportunity for adversaries to plant small bits of malicious code throughout software that remain dormant until activated by transitive dependencies in the cloud. This is a frightening scenario for government, but one grounded in reality. This often occurs when a government employee unwittingly downloads a bit of open source code to solve a problem and inadvertently introduces risk to the organization.

Ultimately, many cybersecurity issues originate from inside agencies. There is a surprising number of people who try to build software for the government and do not pass background checks. Agencies should be screening candidates and vendors must more diligently, because these instances are only increasing.

"The best way to deal with complexity is to give the open source developers the means to deal with complexity, with much better interfaces and concepts and tools."

Using Chat GPT to Code

Panelists agree that using GPT to write code is helpful up to a point, and should not be relied upon to write code for final production. Correct prompting is important, as is reviewing the code for accuracy. Other agencies are using GPT to help with compliance and expedite some of the cybersecurity requirements mandated by the government.

"It's a useful starting point, but you need a more senior person to be able to review it. In the open source world, code can come from anyone, anywhere. GPT is just another source of code."

Final Thoughts

- Open Source is the modern development platform and gives government agencies access to the latest innovation when building applications. However, with that come risks and the need to ensure the software used meets the standards that government agencies might expect.
- Building in automation increases confidence in the development and deployment process.
- There is a big gap between the security capabilities of big and small projects. There are many small projects using open source code that do not have the resources to properly manage the complexities of open source security.
- This is not a Federal issue, this is a worldwide issue. Government and industry must work together to find a solution and minimize risk as much as possible.