open
invention
network®

Enabling freedom of action in Open Source technologies for the world's largest patent non-aggression community.

Open Source Software Security: A Growing Global Concern

DevSecOps divisions are approaching security as an ongoing part of software development and "baking" security into every step of the development cycle.

info@openinventionnetwork.com | Phone: 919-313-4902 | www.openinventionnetwork.com

Open Source Software (OSS) paves the way for new innovations, drives worldwide digital transformation, and impacts the daily lives of individuals and businesses throughout society.

OSS code is available to the public — free for anyone to use, modify, or inspect. As a result, Open Source facilitates collaborative innovation and the development of new technologies to help solve shared problems, which is why critical infrastructure and national security systems incorporate it. However, according to Google, there's not any official resource allocation and only a few formal standards for maintaining the security of Open Source code. In fact, most of the work to maintain and enhance the security of Open Source, including fixing known vulnerabilities, is done on an ad hoc, volunteer basis.

Securing the world's Open Source code should be a collective effort and involve all parties — from programmers, dev ops, businesses of all sizes, to government organizations — involved in the software development ecosystem.

Log4j Vulnerability Gets Attention

Public officials throughout the world have expressed new security concerns around Open Source Software after an employee at China-based Alibaba Group Holding Ltd.'s cloud security team found and reported the Log4j flaw in November 2021. The project — which helps monitor global activity in untold millions of pieces of software code — is maintained by a group of volunteers as part of the Apache Software Foundation. Left unfixed, the flaw could allow hackers to overtake computers remotely, leading to a wide range of other consequences.

Industries and governments have made strides tackling security issues that have affected software in the past, which traditionally has been proprietary software. The Log4j vulnerability demonstrates the need for the same attention — and commitment — to safeguarding Open Source Software.

Cyber Attacks Against Corporate Networks Increased 50%

According to an article in *Security Brief Asia*, cyberattacks against corporate networks increased 50% in 2021. Education and research industries were hit the hardest, averaging 1,605 attacks per week, with government organizations, communications companies, and Internet Service Providers (ISPs) close behind. Even attacks on healthcare were up 71% on pre-pandemic levels, showing nothing is off-limits to threat actors. The Check Point Software "2022 Security Report" also disclosed that email is an increasingly popular way to distribute malware — especially during the pandemic — and now accounts for 84% of malware distribution.

"Beyond the corporate world, it was also clear that large-scale attacks on critical infrastructure, such as the Colonial Pipeline incident, had a very real impact on people's day-to-day lives, even threatening their physical sense of security," says Gary Gardiner, Head of Security Engineering in Asia Pacific and Japan for Check Point Software.

The European Commission Connects the Dots in a New Security Ecosystem

Software security concerns have become such common place, governments in Europe are distributing ads on TV and YouTube, encouraging citizens to run updates on digital devices for enhanced safety and security. The European Commission's Directorate-General for Informatics (DIGIT) has announced a "Bug Bounty Program." Launched on Twitter, DIGIT calls "ethical hackers" to find and fix bugs in specific OSS programs for awards up to 5,000 euros as the European Commission continues to "think open" with its software policies and overarching policy.

Japanese Concerns about OSS Security Come to the Forefront

Many companies and organizations throughout Japan are also prioritizing the subject of security. In fact, the Japanese Ministry of Economy, Trade and Industry (METI) recently created a 5th task force for examining software management methods to ensure cyber security. OIN members — Toyota and NEC — as well as other businesses and academia stakeholders — are actively discussing the security of software, both OSS and proprietary. Topics include Software Bill of Materials (SBOM) and associated formats such as Software Package Data Exchange (SPDX), Software Idention (SWID) tagging and CycloneDX. Linux Foundation's SPDX — which allows the expression of components, licenses, copyrights, security references and other metadata relating to software — has become the International Organization Standard (ISO) for security, license compliance, and other software supply chain artifacts. As an ISO standard, SPDX is viewed to be easier to accept for broad usage by Japanese industry and other parties. For its part, OIN has added SPDX packages into its Linux System definition, so that this software will be covered by the OIN community patent cross-license when Table 11 becomes effective in March 2022.

From the White House: Open Source Security Summit

On January 13th, U.S. President Joe Biden's administration officials met with major tech organizations such as Apple, Alphabet (Google), IBM, Meta, Microsoft, Oracle, and others to discuss improving the security of Open Source projects. The White House Open Source Software Security Summit focused on how to better prevent security defects, improve the process for finding them, and shorten the time it takes to fix faulty code.

Open Source Security Solutions & Possibilities

In a forward-looking interview with *CybersecAsia*, Pierluigi Cau, the Director of Solutions Engineering in Asia Pacific for GitHub, discusses the state of Open Source Development, Security, and Operations (DevSecOps) in his region. He explains DevSecOps divisions are approaching security as an ongoing part of software development and "baking" security into every step of the development cycle. By adopting a "shift-left" approach to security, developers become empowered to continually check for vulnerabilities as part of both the development and testing phases. Understanding dependencies and the risks associated with them, conducting regular checks to remove unnecessary dependencies, and monitoring the entire software development supply chain, are key steps developers need to take as they build secure code.

Not surprisingly, organizations are starting to understand security must be a shared responsibility between developers, security professionals and business leaders, he says. OSS security is not something an individual, or company can manage alone. Organizations, developers and security researchers must come together and commit time, resources, and expertise to find and report vulnerabilities in Open Source Code, build new and improved security tools and create best Open Source security practices for everyone.

Chief Security Officer at GitHub, Mike Hanley, explains just how important OSS is to the commercial software and online services the world uses every day to *TechRadar Pro*. "Open Source Software underpins most of the software we use daily — just one or two lines of vulnerable code can have a global ripple effect across the billions of developers and services that rely on it. As the world's largest developer platform, GitHub takes those risks seriously and understands its responsibility to support the millions of developers on our platform in securing open source. Addressing software supply chain security is a team sport. Through partnerships with governments, academia, developers, and other organizations, we can make a significant impact on the future of software security, and today's discussion is an important step in securing the world's code together."

After attending the White House Open Source Software Security Summit, Google wants a public-private partnership to not only fund, but also staff essential Open Source projects. In a blog post, President of Global Affairs and Chief Legal Officer at Google and Alphabet, Kent Walker lays out the search giant's plans to better secure the OSS ecosystem. "For too long, businesses and governments have taken comfort in the assumption that OSS is generally secure due to its transparent nature," he writes. "While many believe that more eyes watching can help detect and resolve problems in the Open Source community, some projects actually don't have many eyes on them while others have few, or none at all."

Conclusion

Open Source has become the defacto standard with Open Source code the key driver behind most software services and products — far more than proprietary software. Given what is at stake, the Open Source community will need to come together to address security issues. As just one example of more that will follow from the global community, the Open Source Security Foundation recently announced the Alpha-Omega Project to improve software supply chain security for 10,000 OSS projects. On February 1st , Microsoft and Google supported the Alpha-Omega Project with an initial investment of $5 million and committed personnel to jump start the initiative.

At Open Invention Network (OIN), we stand with the Open Source community on improving software supply chain security through process improvement, mindset shifts, and the investment of dedicated resources. This is an area that must be an important priority for everyone that develops or uses Open Source, and that is all of us.