Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

SECURITY CONSIDERATIONS WHEN USING OPEN SOURCE SOFTWARE

July 2020

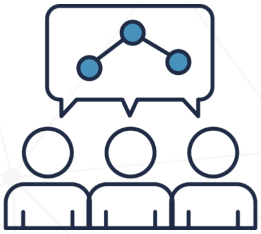
ITSAP.10.059

When looking to acquire software, your organization might consider using open-source software (OSS), as well as commercially available products. OSS has some advantages; because OSS is software that uses publicly available source code, it's affordable and flexible. However, sometimes you get what you don't pay for. While OSS can be convenient, using it can introduce vulnerabilities and security risks to your organization. This document outlines these risks as well as steps you can take to minimize them.

OPEN SOURCE

Open source code is created through voluntary collaboration of software developers. The original authors license the code so that anyone can see it, modify it, and distribute new versions of it. This allows developers to extend open source code to create new stand-alone products or add new functionality to existing software products.

OSS is very common. You are probably already familiar with several open source products, like Google Chrome and Firefox web browsers. Due to the nature of publicly available OSS, anyone can make changes to existing open source code. This accessibility makes it easy to customize OSS to suit your business needs. Capabilities can be added, removed, or modified as needed.



78% of companies run open source software, but less than half are managing it properly

- 2016 Future of Open Source Survey Results

RISKS

Before you implement OSS in your organization, you should consider the associated risks, including the following examples:

- **Excessive access:** Open access means the code is available to all, which creates opportunities for cyber threat actors to manipulate code maliciously. Using OSS can give threat actors opportunities to gain access to your networks and information.
- **Lack of verification:** There are no guarantees that qualified experts conduct proper testing and quality assurance throughout the development of OSS, or that those who review the code thoroughly check its security. This lack of verification can make your IT infrastructure vulnerable.
- **Lack of support:** Most OSS does not have dedicated support. Without a support team, updates and security patches may not be available. If vulnerabilities are discovered in the software, cyber threat actors can exploit these vulnerabilities to gain access to your organization's network, systems, and information. Keep in mind that it is the responsibility of the project community that is maintaining the OSS to report and patch any known vulnerabilities.

Not all OSS carries the same level of risk. In fact, most commercial IT security products have open source components worked into their code. For example, consider companies that manufacture IT security products that offer cryptographic functionality. These manufacturers embed the open source OpenSSL cryptographic library in their product lines.

Before you acquire and implement OSS, it is essential that you conduct assurance activities. With these activities, you can continue to protect the security of your organization's networks, systems, and information.

OSS DEVELOPMENT LIFECYCLE

Open source is a term that refers to a specific approach to creating computer programs. This approach is built on the values of collaboration, transparency, and community-oriented development. The development lifecycle for OSS development lifecycle includes: collecting requirements, designing, implementing, testing, releasing, and maintaining. There are large organizations supporting OSS projects. However, these projects may rely on work conducted by smaller OSS projects that are run by volunteers.

OSS is released to the public as soon as the project team gets it running, even if it contains bugs. OSS often depends on public inspection and review to improve the product over time. Volunteers test the software and then send feedback to report bugs and suggest fixes. The software's project members use this feedback for the new development release of the software. This process happens as many times as needed to improve the software and release stable versions.

In the case of smaller OSS projects, volunteers may have less time to fix problems or conduct security testing. OSS projects may not receive the funding needed to hire expert security auditors. Security is not necessarily incorporated into the design and development of OSS, which may produce vulnerabilities and introduce risks to your organization.

PROTECT YOUR ORGANIZATION

Make sure your organization has an IT security framework. This framework should include the following components:

- **Organizational IT security policy** - A sound IT security policy outlines how employees work and collaborate on corporate networks while respecting the organization's position on managing security risks. Be sure to review and update this policy regularly so that it reflects the current threat environment.
- **Resource allocation** - Define the roles and responsibilities of system administrators, and limit the number of individuals with this level of access.
- **System administration procedures** - Develop procedures that define how system administrators should securely manage and maintain your organization's networks and software.

CONSIDERATIONS FOR USING OSS

Ultimately, OSS should align with your organization's overall IT strategy, but here are some factors to consider when using OSS.

Before acquiring new software: Your organization should determine the level of risk that is tolerable and can be accepted. When your risk tolerance is clearly identified, you can narrow down your choices and pick the software products that support your business needs and security requirements.

Before installing new software: Your organization needs measures to detect and mitigate vulnerabilities, such as logs, audits, and incident response processes. Always test software before installing it, and test software throughout its lifecycle, such as when it needs to be updated or patched. Continuous monitoring and testing can reduce the risk of exploits.

When using OSS: You should manage all OSS using the same procedures and tools that you use for commercial products. As always, train your employees on cyber security best practices that can help them securely use and manage software products.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**