Aptivaa

LEADING THROUGH INNOVATION

# Third Party Software Security

## 1. What is Third Party Software Components?

The usage of third-party software components (TPCs) has significantly increased in the software development processes. These TPCs include both open-source software (OSS) and commercial off-the-shelf (COTS) components that provides libraries and files of common functions allowing developers to focus on product-specific customisations and features. TPCs, used as readymade building blocks, enable faster time to release the product in the market and lower development costs.

## 2. Key challenges associated with using third-party components:

Many enterprises end up using software packages that include third-party dependencies which may not have been well managed or may be susceptible to various vulnerabilities which could be easily exploited.

- **1. Bill of Materials for third-party software components**

- Identification of the third-party components along with establishing and maintaining the bill of materials (BOM) is the first step to implement good software security hygiene but there are significant challenges as detailed further:

- Automated solutions and tools are available that identify third-party components and generate a BOM; however, there is not a one-size-fits-all solution. A company that uses several different programming languages and frameworks would require a tool that understands all of them to be able to find all the included TPCs.

- Due to inaccurate BOM, including third-party component names and multiple versions, it is very difficult to identify new or existing vulnerabilities and the corresponding patches correctly and consistently. Even when new security vulnerabilities are published, organisations scramble to identify which of their products, if any, are affected.

### 2. Naming of Components

- Third-party software components are not uniquely identified. Unfortunately, a single TPC is sometimes known by multiple names, and it can be difficult to find the correct or most commonly used name. For instance, Apache Xerces is often short for Apache Xerces/J, which is also xercesImpl.jar.

- Lack of unique identifiers or inconsistent nomenclature for third-party components originate both outside and inside an organisation.

  1. Outside an organisation, there is no standard naming convention for TPCs, and names vary significantly across software suppliers and communities.
  2. Inside an organisation, the absence of a company-wide naming convention results in different development teams naming the same TPC differently.

### 3. Dependencies

- The hierarchical nature of TPCs further complicates the identification of TPC.
- A single TPC may use several TPC sub-components, each of those further referencing additional TPC sub-components, and so on.

### 4. Vulnerability

- Often, products will utilize a subset of the functionality contained in a TPC and it will be affected by Common Vulnerabilities and Exposures (CVE). The contents of the CVE may not be sufficient for a team to quickly determine whether its usage of a component is affected.
- When a new security vulnerability is reported for a TPC, development teams are faced with the challenge of determining below:
  1. whether that TPC is included in their product.
  2. whether the product is affected by the vulnerability.

## 3. Numbers

- The number of packages hosted by the major ecosystems has grown significantly — by 20% in the last year, according to a report published by software security firm Sonatype.
- The security of open-source software projects overall has improved over the past decade, with the average time to update vulnerable code dropping to 28 days in 2021 compared with 371 days a decade ago.
- Attackers are heavily focused on open-source projects to attack the developers and companies that use the software components, with the number of attacks documented by the firm increasing by more than 650% in 2021.
- The top four ecosystems — Java, JavaScript, .NET, and Python — grew by a combined 20%, churning out 6.3 million new versions and adding almost 724,000 brand-new projects.
- The four most popular software ecosystems grew to 37 million downloadable package versions.

## 4. Security Risks

- Product teams and developers often select third-party components purely based on the functionality they deliver, without considering the security, supportability, and maintainability of these components.
- Most developers connect to a repository, and download the latest software versions of packages without considering

whether those packages were scanned for vulnerabilities?

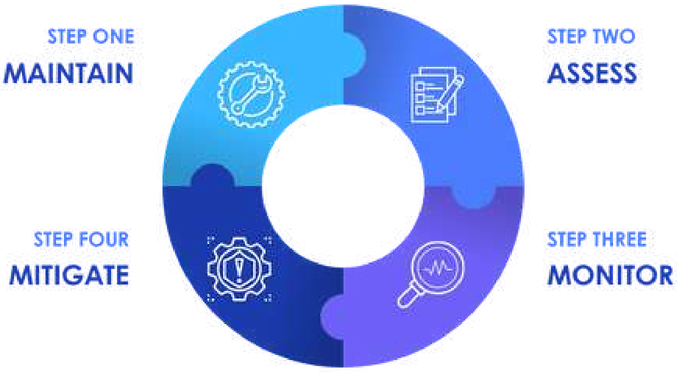
- The AI/ML Factor: As companies increasingly pursue analytics based on artificial intelligence and machine learning (AI/ML), they are facing similar challenges since a great deal of the algorithms are open-source which are actively developed and updated.

- Some third-party components may not have been designed or implemented with security in mind, resulting in the following security risks that could affect the products or services that use them.

  - Downtime of critical systems/network resources.
  - Loss of customer trust and relationship (as is the case when a breach occurs).
  - Loss of confidential and personally identifiable data.
  - Network Intrusion
  - IP Theft

## 5. Managing the TPC

- The overall TPC life cycle management process is shown below:



### 1. Maintain a List of TPCs:

Identifying a list of TPCs in use or to be used is the first step. It is similar to having a bill of materials, with the key difference that it should include TPCs slated for future use as well as those in current use.

**Key Actions**

- Define a unique identifier
- Map component names
- Create Bill of materials

### 2. Assess Security Risks from TPCs:

Once the list of TPCs is identified, the TPCs should be assessed to identify and evaluate the risks. Determining known security vulnerabilities of a TPC and their impact on the TPCs provides insight into potential risks. The risk assessment should consider aspects that could hint at unknown and potential security risks or legacy issues in using a TPC. These aspects should include assessing the maturity of the TPC provider, such as maintenance cadence, performance stability of the TPC over time, development practices employed by the TPC provider, whether the TPC will reach end of life within the expected lifetime of a product, etc.

**Key Actions**

- Assess known vulnerabilities practices
- valuate component operational risks

### 3. Mitigate or accept risks:

Once the risks are evaluated, an organisation should decide whether its use is acceptable or whether risk mitigation controls need to be implemented.

**Key Actions**

- Patch / Update version
- Replace with equivalent component
- Branch code internally
- Contribute to community/vendor
- Mitigate through code.
- Accept risks

### 4. Monitor for changes:

Once a TPC is incorporated into a product, it needs continuous monitoring to ensure that its risk profile remains acceptable over time. Discovery of new vulnerabilities in a TPC or the TPC reaching the end of life are scenarios that may tip the TPC's risk profile to an unacceptable level of risk.

**Key Actions**

- Respond to new vulnerabilities
- Monitor for end of life
- Communicate risk profile changes
- Respond to policy change

# Contact:

**Sandip Mukherjee**
Co-Founder,
Aptivaa
Email - sandip.mukherjee@aptivaa.com

**Mayur Muzumdar**
Director - Practice Head Cyber Risk Services,
Aptivaa
Email - mayur.muzumdar@aptivaa.com

**Vivek Gupta**
Director - Client Relationship,
Aptivaa
Email - vivek.gupta@aptivaa.com

Aptivaa

Aptivaa is a vertically focused finance and risk management consulting and analytics firm with world-class competencies in Credit Risk, Market Risk, Operational Risk, Basel III, IFRS9, Risk Analytics, COSO, ALM, Model Risk Management, ICAAP, Stress Testing, Risk Data, Cyber Risk Services and Reporting. Aptivaa has emerged as a leading risk management solutions firm having served over 100 clients across 22 countries comprising of highly respected names in the financial services industry.

www.linkedin.com/company/aptivaa | @AptivaaTV

Disclaimer:
This publication contains general information only. Aptivaa by means of this publication is not rendering any services or professional advice. This publication should not be used as a basis for any decision or action. Aptivaa and none of its entities shall be held liable or responsible for any loss whatsoever sustained by relying on this publication.