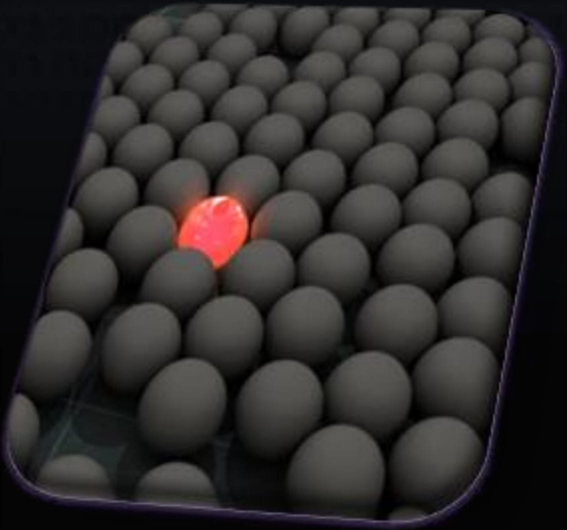
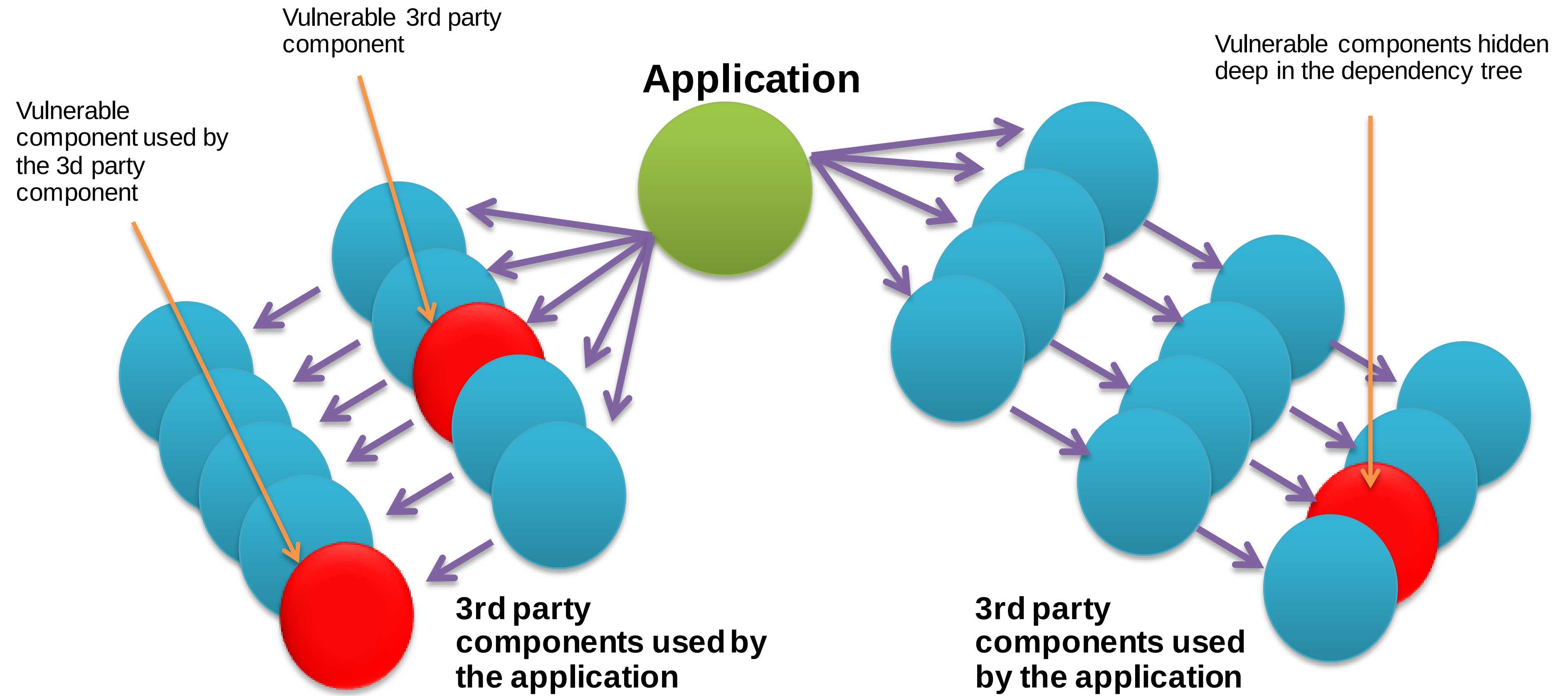
# Using Components with Known Vulnerabilities

CYBER SECURITY & PRIVACY FOUNDATION

# Introduction



- When creating an application, developers often make use of existing third-party libraries or frameworks to speed up the development and improve the efficiency and quality.
- But, it creates a way for vulnerable code to sneak into our secure application.
- A vulnerable components leaves the application vulnerable to hackers


Vulnerable 3rd party component
Vulnerable component used by the 3d party component
Application
Vulnerable components hidden deep in the dependency tree
3rd party components used by the application
3rd party components used by the application

In Many cases, developers don’t even know the list of third-party components used in their application.

Developers often don’t aware the components used in their application are known to be vulnerable.

Vulnerable components can cause almost any type of security risks.

Components most often have high privilege in the application, causes potential security risk(Ex: Remote code Execution).

# Vulnerabilities in Very Popular Libraries

# Apache Struts 2

**Apache Struts 2** is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model–view–controller (MVC) architecture.

## Vulnerabilities

**CVE-2013-2251:** Multiple Remote Command Execution (Apache Struts 2.0.0 prior to 2.3.15.1 )

**CVE-2014-7809:** bypass cross-site request forgery protections

**CVE-2013-4316:** Remote code-execution vulnerability (Versions prior to Apache Struts 2.3.15.2)%

# Spring Framework

The Spring Framework provides a comprehensive programming and configuration model for modern Java-based enterprise applications - on any kind of deployment platform.

**CVE-2011-2730:**
Allows attackers to perform Expression Language Injection

**Versions Affected:**
3.0.0 to 3.0.5
2.5.0 to 2.5.6.SEC02 (community releases)
2.5.0 to 2.5.7.SR01 (subscription customers)
Earlier, unsupported versions may also be affected

# Apache CXF Framework

Apache CXF is an open source services framework. CXF helps you build and develop services using frontend programming APIs, like JAX-WS and JAX-RS.

**CVE-2012-2379:**

By failing to provide an identity token, attackers could invoke any web service with full permission.

**Affected:**

Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1

# Defence

- Identify all used third-party components(including their dependencies) and their versions.
- Monitor the security of these components in public databases, project mailing lists, and security mailing lists.
- Keep the components to date.
- Remove unused components
- Establish security policies governing component use, such as requiring certain software development practices, passing security tests, and acceptable licenses.

# Tools

✓ Contrast Security – real time continuous monitoring for known and unknown vulnerabilities

✓ Sonatype – management for development organization policy enforcement

✓ OWASP Dependency Check – open source tool to analyze an application’s components