How To Keep Your Dependencies Secure And Up-To-Date

Pramod Rana (@IAmVarchashva)
About Me

• Manager - Application Security @Netskope
• Security Testing & DevSecOps
• Open Source Products - vPrioritizer and Omniscient
• Speaker at BlackHat, Defcon, nullcon & Grayhat | OWASP Pune Chapter Lead
In last 10 years or so, software development process has evolved. Safe to say that softwares are assembled now, more than developed. These pieces (open source in most cases) of software brings new set of security challenges. Hint - log4j ;)

Flexibility is great for development, bad for security.

<table>
<thead>
<tr>
<th>Software Composition Oversimplified</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;10 years back</td>
</tr>
<tr>
<td>Someone else’s code</td>
</tr>
<tr>
<td>Organization owned code</td>
</tr>
<tr>
<td>Now</td>
</tr>
<tr>
<td>Organization owned code</td>
</tr>
<tr>
<td>Someone else’s code</td>
</tr>
</tbody>
</table>
(In)Security Landscape

- Open source code is integral part of supply chain for *almost* all softwares
- Vulnerability affecting open source code has impact on industry scale
- Given enough eyes, no code is secure
Solution Outline

• Inventory / SBoM of all 3rd party code (more often open source)
• How many components has known vulnerabilities. In almost all cases, ALL
• If and how organization is affected by those vulnerabilities
Methodology

- **Github Dependabot** is one of the solutions to detect whether our dependencies are secure and up-to-date.
- Dependency graph module helps in identifying the 3rd party code usage (**supported packages**).
- Dependabot alerts module identifies security vulnerabilities affecting used 3rd party code and creates a pull request to upgrade the vulnerable package, if available.
Pull Request Monitoring Automation

- Monitors the pull requests created by Dependabot and feed it back to Jira into the right teams bucket, where developers can triage and remediate it holistically along with other areas of work
- Enables the Dependabot security alerts for all unarchived repositories, if not enabled already

We are in process of providing the framework as open source solution
Thank you!

My coordinates - [LinkedIn](#) | [Twitter](#) (@IAmVarchashva)