Jeremiah Kellam

CSD380 Module 11.1 Discussion

7/18/2024

Dependency Scanning:   
when it should be used,   
why it should be used, and  
what tools are available, if any, to help with implementation.

Hello,

For the Module 11 discussion I will be covering the topic of Dependency Scanning and addressing items like when it should be used, why it should be use, and what tools are available to help with implementation. To start, Dependency Scanning involves the detection and management of third-party libraries or modules in your code that it depends on. It makes sure that the libraries and modules are secure and up-to-date (Benhassen). Dependency Scanning should be used on a regular basis during development and especially before deploying a product to market to make sure that modules and libraries that your code is dependent on are current and safe.

Everything that is external to your build can be an avenue for a new risk to be introduce, this is why it is important to perform dependency scanning. These vulnerabilities that are inherent in something you are relying on could compromise your own work. So, scan regularly and fill the gaps. Certain risks that could be eliminated are old libraries, transitive dependencies that have their own dependencies, and licensing that certain dependencies may create conflict or legal issues in their use (Starita). Some tools are available to help with dependency scanning like [Mend.io](https://www.mend.io/) (formerly WhiteSource) that is a platform which manages open-source security and keeps you compliant. There is also GitLab and it is a platform that includes dependency scanning as well as having a very well laid out SOP on how to set it up, look here: [Tutorial: Set up dependency scanning | GitLab](https://docs.gitlab.com/ee/tutorials/dependency_scanning.html). OWASP [Dependency-Track](https://dependencytrack.org/) is an intelligent component analysis platform that uses the Software Bill of Materials to look for vulnerabilities (OWASP). Hope this coverage on the topic was interesting and informative.

Thank you for your time,

Jeremiah K.

Reference(s):

Benhassan, T. (2024, April 21). Improve Your Code Security with Dependency Scanning. Medium. <https://medium.com/@tamerbenhassan/improve-your-code-security-with-dependency-scanning-47f509111261>

Starita, A. (2024, July 12). Dependency Management: Protecting your code. <https://www.mend.io/blog/dependency-management-protecting-your-code/>

OWASP Foundation. (n.d.). OWASP Dependency-Track. <https://owasp.org/www-project-dependency-track/>