Making Invisible Things Visible: Tracking Down Known Vulnerabilities at 3000 Companies (Showcase)

Gazi Mahmud

Sonatype, USA

gmahmud@sonatype.com

ABSTRACT

This year, software development teams around the world are consuming BILLIONS of open source and third-party components. The good news: they are accelerating time to market. The bad news: 1 in 17 components they are using include known security vulnerabilities. In this talk, I will describe what Sonatype, the company behind The Central Repository that supports Apache Maven, has learned from analyzing how thousands of applications use open source components. I will also discuss how organizations like Mayo Clinic, Exxon, Capital One, the U.S. FDA and Intuit are utilizing the principles of software supply chain automation to improve application security and how organizations can balance the need for speed with quality and security early in the development cycle.

CCS Concepts

• Security and privacy→Vulnerability management • Software and its engineering→Software creation and management *• Security and privacy→Software security engineering • Security and privacy→Web application security*

Keywords

Software Component Lifecycle Management; Continuous Integration; DevOps; OSS Repository Hosting; OSSRH; Sonatype; The Central Repository; Nexus Repository OSS; Nexus Firewall; Open Source Software; Software Variability Management

BIOGRAPHY

Gazi Mahmud is a Senior Data Scientist and Lead Architect at Sonatype where he is responsible for the Technical Vision for innovation and Architecture Design for data pipeline pertinent to component intelligence and Software Supply Chain principles. He has 17 years of experience in Enterprise Software as a Service (SaaS) Architecture, and in Information Retrieval theories and practices across the facets of Big Data ecosystems. He holds an MS in Computer Science and a dual Bachelors degree in Applied Mathematics and Computer Science from University of California, Berkeley.

FSE'16, November 13–18, 2016, Seattle, WA, USA
ACM. 978-1-4503-4218-6/16/11...$15.00
http://dx.doi.org/10.1145/2950290.2994155