Wednesday, February 16, 2022
11:00 AM – 11:20 AM
Log4j Lessons for the Source Code Vulnerability Killchain (and How to Protect Your Organization)

Peter Shin
CEO/Founder
Canvass Labs, Inc.

Abstract:
Software is the glue that connects people and systems, across every industry, and enables them to solve problems. Given its pervasiveness, even if your organization does not produce its own software, you can no longer afford to ignore the associated cybersecurity risks.

Just like modern manufacturing, software developers reuse existing third-party components to reduce costs. A custom software project can incorporate hundreds of such third-party components, forming a software supply chain. The most popular third-party software components are used in thousands of applications, including defense and critical infrastructure, and can present a global Achilles heel. When a vulnerability is discovered, such as the recent Java log4j vulnerability, the blast radius can be huge.

For software consumers, typical Information Technology (IT) services are insufficient: an explicit cybersecurity strategy must be developed within the organization. Stakeholders must be educated to understand the impact of security risks. Vendors should be questioned regarding the provenance of third party software components within deliverables, and their own risk mitigation practices.

Key elements of a strong cybersecurity strategy include:

1) Assessment: How well do you know the software deployed in your organization?

2) Risk Identification: What is at stake if a system is compromised or becomes unavailable?

3) Resourcing: How much money and manpower should you invest to protect your organization, and how best to utilize that budget?

For software producers, the process is no longer fire-and-forget. Security threats must be monitored in the software supply chain even after a project has been delivered, and updates provided to eliminate them. A DevSecOps (Development, Security, and Operations) approach to software development is required because security is considered throughout the software lifecycle, not just at the end, and not just once. Improving how third-party software risk is assessed, and software supply chain information is managed, are critical elements of DevSecOps.

A variety of tools exist for identifying the software components used in a project (aka Software Composition Analysis or SCA), and public databases of known software vulnerabilities are available. Tools that integrate this information to produce risk assessments should be integrated into software development and management practices. Having such tools and processes in place can form a source code vulnerability killchain, to rapidly identify and respond to newly discovered cybersecurity threats. Canvass Labs is currently exploring the use of artificial intelligence (AI) for source code vulnerability detection, as part of a greater system for software supply chain risk mitigation, through a Department of

Defense (DoD) Small Business Innovation Research (SBIR) award. Such systems can help contractors deliver safer software solutions, help organizations vet the security of outsourced deliverables, and improve the security posture of in-house software development efforts.