Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security

May 26, 2021

Workday appreciates the opportunity to provide feedback on the National Institute of Standards and Technology (NIST) call for position papers related to standards and guidelines to enhance software supply chain security.

Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organizations around the world and across industries—from medium-sized businesses to more than 45 percent of the Fortune 500.

Workday welcomes the recognition within the *Executive Order (EO) on Improving the Nation's Cybersecurity* of the benefits of secure cloud service and the call for federal agencies to prioritize the adoption and use of cloud technology. In addition, given its long track record of stakeholder engagement and collaboration, we are pleased to see NIST play a central role in the development and implementation of the EO directives. We are pleased to provide the following information related to the five areas that NIST specified.

1. *Criteria for designating "critical software."*

Workday defines software that runs within production customer environments, as well as software outside our production customer environments that enables its services to function, as both business-critical and security-critical. These critical software services must be highly reliable and performant in order to meet the business needs of our customers while ensuring the continuous security of customer data.

As NIST considers criteria for the designation of software as critical, Workday encourages an emphasis on factors that trigger the designation at a certain date in order to maximize predictability versus factors that trigger the designation subsequent to implementation (*e.g.*, scale of use).

2. *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.*

Workday has implemented a risk-based, secure software development framework that is integrated within the development lifecycle to ensure the outcome of secure software and products. The framework and associated policies, standards, and guidelines are based on industry best practices and globally recognized frameworks, such as NIST SSDF, and describe security requirements for each stage of the software development lifecycle (SDLC), from design to deployment. The end-to-end engagement within the development lifecycle ensures that new services or changes to existing services are risk assessed and that appropriate security controls and requirements are implemented prior to/post deployment. Key security practices are conducted in collaboration with the development, program, and product management teams and include but are not limited to, security risk assessment, establishment of secure design requirements and architecture diagrams, threat modeling, static code analysis, open source software composition analysis, dynamic code analysis, and internal/external penetration testing.

3. *Guidelines outlining security measures that shall be applied to the federal government's use of critical software.*

As part of Workday's secure software development framework, key security measures and requirements have been outlined for new and existing services. These include, but are not limited to implementing secure authentication and authorization methods (RBAC, least privilege, etc.); logging and auditing of key user activity, events, and state-changing operations; data security (data isolation, encryption standards, etc.), secure network design and connectivity; service resilience and availability; standardized service deployment model (configuration management, change management, etc.); and secure and compliant usage of open source software.

4. *Initial minimum requirements for testing software source code.*

Workday conducts automated testing of software source code, utilizing tools and practices, such as static code analysis and open source software composition analysis to identify, triage (risk rank and prioritize), and remediate internal and/or 3rd party security flaws prior to deployment. Additionally, software features deemed as higher risk (based on risk assessment) are manually assessed prior to production release through formal security architecture reviews, code reviews, and internal and/or external penetration tests. After initial deployment, the aforementioned security controls are performed on a continuous and repeatable basis, with the addition of dynamic code analysis. At the right-most element of Workday's secure software development framework is a public Bug Bounty program. The program provides an additional layer of security, where security flaws are identified and privately reported by external researchers. Any reported security issues are promptly reviewed, triaged, and actioned by internal development and security teams.

5. *Guidelines for software integrity chains and provenance.*

Workday continues to mature our software integrity practices and has established/working to establish a number of sourcing, access, and integration controls for software components prior to product delivery. Key guidelines within scope include, but are not limited to: a formal sourcing/procurement process with integrated 3rd party risk management; strong physical security; least privileged access across development and build systems; open source software governance (includes licensing compliance and SBOM); static and dynamic code analysis; internal/external penetration testing; change and configuration management; separation of duties/environments; and logging and monitoring.

Workday appreciates the opportunity to provide this feedback related to software security standards and guidelines. We look forward to the process moving forward and the upcoming workshop focused on enhancing software supply chain security. Please do not hesitate to reach out to Chandler C. Morse at chandler.morse@workday.com for further assistance.