PROJECTS

Secure Software Development Framework SSDF

PROJECT LINKS

Overview

NIST has finalized SP 800-218A, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile*. This publication augments SP 800-218 by adding practices, tasks, recommendations, considerations, notes, and informative references that are specific to AI model development throughout the software development life cycle. The Profile supports Executive Order (EO) 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

To gather input for SP 800-218A in support of EO 14110, NIST held a virtual workshop on **Secure Development Practices for AI Models** on January 17, 2024. A recording of the workshop can be viewed on NIST's website.

NIST Special Publication (SP) 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* has been posted as final, along with a Microsoft Excel version of the SSDF 1.1 table. SP 800-218 includes mappings from Executive Order (EO) 14028 Section 4e clauses to the SSDF practices and tasks that help address each clause. Also, see a summary of changes from version 1.1 and plans for the SSDF.

The Secure Software Development Framework (SSDF) is a set of fundamental, sound, and secure software development practices based on established secure software development practice documents from organizations such as BSA, OWASP, and SAFECode. Few software development life cycle (SDLC) models explicitly address software security in detail, so practices like those in the SSDF need to be added to and integrated with each SDLC implementation.

Following the SSDF practices should help software producers reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent recurrences. Also, because the SSDF provides a common language for describing secure software development practices, software producers and acquirers can use it to foster their communications for procurement processes and other management activities.

Back to Top

SSDF Practices

The SSDF practices are organized into four groups:

- **Prepare the Organization (PO)**: Ensure that the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.
- **Protect the Software (PS)**: Protect all components of the software from tampering and unauthorized access.
- **Produce Well-Secured Software (PW)**: Produce well-secured software with minimal security vulnerabilities in its releases.
- **Respond to Vulnerabilities (RV)**: Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.

Each practice is defined with the following elements:

- **Practice**: The name of the practice and a unique identifier, followed by a brief explanation of what the practice is and why it is beneficial.
- **Task**: An action that may be needed to perform a practice.
- **Notional Implementation Example**: A notional example of types of tools, processes, or other method that could be used to help implement a task. No examples or combination of examples are required, and the stated examples are not the only feasible options.
- **Reference**: A pointer to an established secure development practice document and its mappings to a particular task.

SSDF version 1.1 is defined in NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.* NIST SP 800-218 replaces the NIST Cybersecurity White Paper, *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* that defined SSDF version 1.0.

Back to Top

SSDF Use

The SSDF can help an organization to align and prioritize its secure software development activities with its business/mission requirements, risk tolerances, and resources. The SSDF's practices are outcome-based. Comparing the outcomes an organization is currently achieving to the SSDF's practices may reveal gaps to be addressed. An action plan to address these gaps can aid in setting priorities that take into consideration the organization's mission and business needs and its risk management processes.

In addition to **risk**, factors such as **cost**, **feasibility**, and **applicability** should be considered when deciding which SSDF practices to use and how much time and resources to devote to each practice. **Automatability** is an important factor to consider, especially for implementing practices at scale. Also, some practices are more advanced than others and have **dependencies** on certain foundational practices already being in place.

The SSDF's practices, tasks, and implementation examples represent a starting point to consider; they are meant to be changed and customized, and to evolve over time. The intention of the SSDF is not to create a checklist to follow, but instead to provide a basis for planning and implementing a risk-based approach to adopting secure software development practices and continuously improving software development.

Back to Top

New in Version 1.1

The most noteworthy changes in SSDF from the original to version 1.1 are:

- **Practices**: Added PO.5, "Implement and Maintain Secure Environments for Software Development"
- **Tasks**:
  - Added PO.1.2 on documenting security requirements for organization-developed software to meet
  - Added PS.3.2 on collecting and sharing provenance data for all components of software releases
  - Added PW.1.2 on tracking software security requirements, risks, and design decisions
- **Notional Implementation Examples**:
  - Added numerous examples suggested in public comments
  - Numbered the examples for each task
- **References**: Added 11 references, including
  - Cloud Native Computing Foundation, Software Supply Chain Best Practices
  - International Electrotechnical Commission (IEC), Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1
  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Information technology – Security techniques – Vulnerability disclosure, ISO/IEC 29147:2018, and Information technology – Security techniques – Vulnerability handling processes, ISO/IEC 30111:2019
  - NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP 800-161 Revision 1
  - Open Web Application Security Project, OWASP Software Component Verification Standard, Version 1.0
- **Other**: Created Appendix A, which maps Executive Order (EO) 14028 Section 4e clauses to the SSDF practices and tasks that help address each clause

For more details, see the change log in Appendix C of SP 800-218. The SP 800-218 landing page also includes supplemental files showing the significant changes from the original SSDF version 1.0 white paper and from the SP 800-218 public draft.

Back to Top

NIST Plans

NIST has been considering next steps for the evolution of the SSDF. It will be updated periodically to reflect your inputs and feedback, and we encourage you to share your thoughts with us as you implement the SSDF within your own organization and software development efforts. Having inputs from a variety of software producers will be particularly helpful to us in refining and revising the SSDF.

Additional actions under consideration include the following:

- Moving reference mappings to an interactive online repository for ease of use and to provide a machine-readable format
- Illustrating how the SSDF can be applied to particular SDLC models, especially transitioning DevOps implementations to DevSecOps **(**for more information on this, see the NIST DevSecOps project site)
- Developing an SSDF baseline targeting open-source software (leveraging the fundamental practices and tasks, and augmenting them with open-source specific examples)
- Developing a practical demonstration of the use of the SSDF for a specific software development model, languages, technologies, etc. for open-source software

Back to Top

Contact Us

Your comments and suggestions for the SSDF project are always welcome. Contact us at ssdf@nist.gov.

Back to Top

ADDITIONAL PAGES

References

CONTACTS

SSDF Inquiries
ssdf@nist.gov

GROUP

Computer Security Division

TOPICS

Security and Privacy: systems security engineering, vulnerability management

Technologies: artificial intelligence, software & firmware

Laws and Regulations: Executive Order 14028, Executive Order 14110

RELATED PROJECTS

Cybersecurity Framework
DevSecOps
National Initiative for Cybersecurity Education
National Software Reference Library
National Vulnerability Database
OLIR
SAMATE: Software Assurance Metrics And Tool Evaluation
Software Identification Tagging
Systems Security Engineering (SSE) Project
Vulnerability Disclosure Guidance

Created February 25, 2021, Updated July 30, 2024

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications?

Subscribe

Contact Us | Our Other Offices

Send inquiries to csrc-inquiry@nist.gov