SLSA, What's Changed in Version 1.0

Jie Kang
Red Hat

2023-05

Red Hat

Agenda

What is SLSA

Changes

- Versioning
- Tracks & Levels
- Core Specification & Verification
- Provenance

What’s next at Adoptium

What is SLSA

Supply Chain Levels for Software Artifacts

slsa.dev

“a security framework, a checklist of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure”

Changes for v1.0

Versioning

V1.0 is the first stable release. Future versions will follow semantic versioning

Backwards incompatible changes increment the major version:

2.0, 3.0, and onwards

Backwards compatible changes increment the minor version:

1.1, 1.2, and onwards

Editorial changes will not result in a version increase

Tracks & Levels

General Levels replaced by Tracks

SLSA Level 1-4

Build Levels 0-3

(Future) Build Level 4

(Future) Source Levels

Core Specification

The core specification has been heavily revised to be easier to understand and apply

- Better terminology
- Rewritten security levels
- Specification updated for producing artifacts, distributing provenance, verifying artifacts, verifying build platforms, and threats & mitigations

Verification

The need for verifying provenance is now included in v1.0

- Establish trust in build platforms
- Establish trust in artifacts

Provenance

New provenance format aimed at addressing rigidity of previous format

The verification summary attestation has also been updated

What’s next at Adoptium

SLSA Attestation

We will work to follow the SLSA Verification Summary Attestation to meet at least SLSA Build Level 3

We will continue to follow updates to the SLSA specification and try to meet all requirements

Build Levels

L1: Provenance exists

L2: Hosted Build Platform

L3: Hardened Builds

L1 and L2 are met

Build L3

Build platform implements strong controls to:

- prevent runs from influencing one another, even within the same project.
- prevent secret material used to sign the provenance from being accessible to the user-defined build steps.

SLSA Attestation

We will work to follow the SLSA Verification Summary Attestation to meet at least SLSA Build Level 3

We will continue to follow updates to the SLSA specification and try to meet all requirements

Thank you