Debido a que los ataques a la cadena de suministro de software están emergiendo como un punto de preocupación a raíz de los incidentes de seguridad de SolarWinds y Codecov, Google propone una solución para garantizar la integridad de los paquetes de software y evitar modificaciones no autorizadas.

Llamado «Niveles de cadena de suministro para artefactos de software» (SLSA), el framework de un extremo a otro tiene como objetivo asegurar el desarrollo y la implementación de software, es decir, el flujo de trabajo de origen, compilación, publicación, y mitigar las amenazas que surgen de la manipulación del código fuente, la plataforma de compilación y el repositorio de artefactos en cada eslabón de la cadena.

Google dijo que SLSA está inspirado en el propio mecanismo de ejecución interno de la compañía llamado Autorización Binaria para Borg, un conjunto de herramientas de auditoría que verifica la procedencia del código e implementa la identidad del código para asegurarse de que el software de producción implementado esté debidamente autorizado y revisado.

> *«En su estado actual, SLSA es un conjunto de pautas de seguridad que se pueden adoptar gradualmente y que se establecen por consenso de la industria»,* dijo Kim Lewandowski, del equipo de seguridad de código abierto de Google, en conjunto con Mark Lodato, de Autorización Binaria para Borg.

> *«En su forma final, SLSA se diferenciará de una lista de mejores prácticas en su aplicabilidad: apoyará la creación automática de metadatos auditables que pueden ser alimentados a motores de políticas para otorgar certificación SLSA a un paquete o plataforma de construcción en particular»,* agregaron.

El marco SLSA promete integridad de la cadena de suministro de software de un extremo a otro y está diseñado para ser incremental y procesable. Comprende cuatro niveles diferentes

de sofisticación de seguridad de software progresiva, y SLSA 4 ofrece un alto grado de confianza en que el software no ha sido manipulado de forma incorrecta.

- SLSA 1: Requiere que el proceso de construcción esté completamente programado/automatizado y genere procedencia
- SLSA 2: Requiere el uso de control de versiones y un servicio de compilación alojado que genera procedencia autenticada
- SLSA 3: Requiere que la fuente y las plataformas de construcción cumplan con estándares específicos para garantizar la auditabilidad de la fuente y la integridad de la procedencia
- SLSA 4: Requiere una revisión de dos personas de todos los cambios y un proceso de construcción hermético y reproducible

> *«Los niveles más altos de SLSA requieren controles de seguridad más estrictos para la plataforma de compilación, lo que hace que sea más difícil comprometer y ganar persistencia»,* dijeron Lewandowski y Lodato.

Aunque el SLSA 4 representa el estado final ideal, los niveles inferiores brindan garantías de integridad incrementales, al mismo tiempo que dificultan que los malos actores permanezcan ocultos en un entorno de desarrollador vulnerado por períodos prolongados.

Junto con el anuncio, Google compartió detalles adicionales sobre los requisitos de origen y compilación que deben cumplirse, y también pide a la industria que estandarice el sistema y defina un modelo de amenazas que detalle las mismas específicas que SLSA espera abordar a largo plazo.

> *«Alcanzar el nivel más alto de SLSA para la mayoría de los proyectos puede ser difícil, pero las mejoras incrementales reconocidas por niveles más bajos de SLSA*

> *ya contribuirán en gran medida a mejorar la seguridad del ecosistema de código abierto»*, dijo la compañía.