Bring Your Lunch, We'll Bring Our Notebooks: Securing Software Workflows

Tabatha DiDomenico, G-Research Open Source
Kadi McKean, ReversingLabs
Stacey Potter, OpenSSF
Katherine Druckman, JetBrains

Tabatha DiDomenico
OSS Security Engineer, G-Research

Kadi McKean
OSS Community Manager, ReversingLabs

Stacey Potter
Community Manager, OpenSSF

Katherine Druckman
Head of Community & Partnership Engagement, JetBrains

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Mission

The Open Source Security Foundation (OpenSSF) seeks to make it easier to **sustainably secure the development, maintenance, release, and consumption of the open source software (OSS).** This includes fostering collaboration within and beyond the OpenSSF, establishing best practices, and developing innovative solutions.

Vision

OSS is a digital public good and as an industry, we have an obligation to address the security concerns with the community. **We envision a future where OSS is universally trusted, secure, and reliable.** Producers of OSS (of all skill levels) have the ability to proactively and retroactively address both existing and emergent security threats through low-friction tooling automation, education, and clear and actionable guidance. This collaborative vision enables individuals and organizations in a global ecosystem to confidently leverage the benefits and meaningfully contribute back to the OSS community.

Source & Repository Security

Dependency Selection & Vulnerability Data

Build & Provenance

Packaging, Signing & Attestations

Distribution & Release

Deploy, Runtime & Secrets

Policy & Platform

Making the Case to Leadership

OpenSSF Working Groups

AI/ML Security

BEAR

Belonging, Empowerment, Allyship, and Representation

BEST

Best Practices for Open Source Developers

Global Cyber Policy

ORBIT

Open Resources for Baselines, Interoperability, and Tooling

Securing Software Repositories

Security Tooling

Supply Chain Integrity

Vulnerability Disclosures

Visit the Working Groups page at https://openssf.org/community/openssf-working-groups/ for information on each group.

OpenSSF Projects

Best Practices Badge

bomctl

gittuf

GUAC

OpenSSF Scorecard

OpenVEX

RSTUF

S2C2F

SBOMit

Sigstore

SLSA

Zarf

OSPS Baseline

Protobom

Minder

OpenBao

Fuzz Introspector

Model Signing

OSV Schema

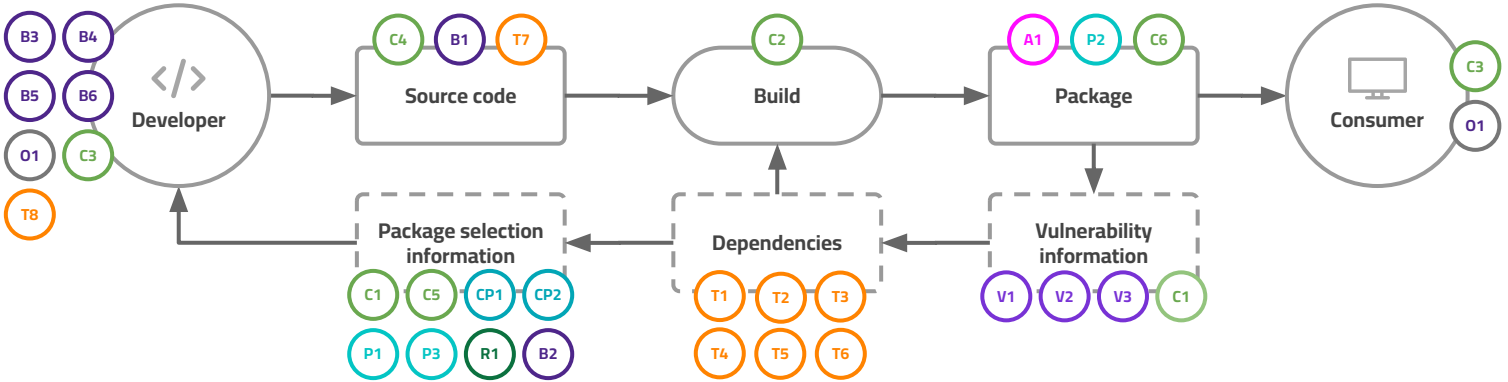
Security Insights

Package Analysis

Criticality Score

https://openssf.org/projects

OpenSSF Technical Initiatives Landscape



Best Practices
B1. OpenSSF Best Practices Badge project
B2. OpenSSF Scorecard project
B3. Education SIG
B4. Memory Safety SIG
B5. C/C++ Compiler Options SIG
B6. Python Hardening SIG

Global Cyber Policy

DevRel Community

AI/ML Security
A1. Model Signing SIG & Project

Supply Chain Integrity
C1. Security Insights project
C2. SLSA project
C3. S2C2F project
C4. Gittuf project
C5. GUAC project
C6. Zarf project M

BEAR (Belonging, Empowerment, Allyship, and Representation)

Securing Software Repositories
R1. RSTUF Project

Security Tooling
T1. SBOM Everywhere SIG
T2. OSS Fuzzing SIG
T3. SBOMit project
T4. Protobom project
T5. bomctl project
T6. Fuzz Introspector project
T7. Minder project
T8. OpenBao project

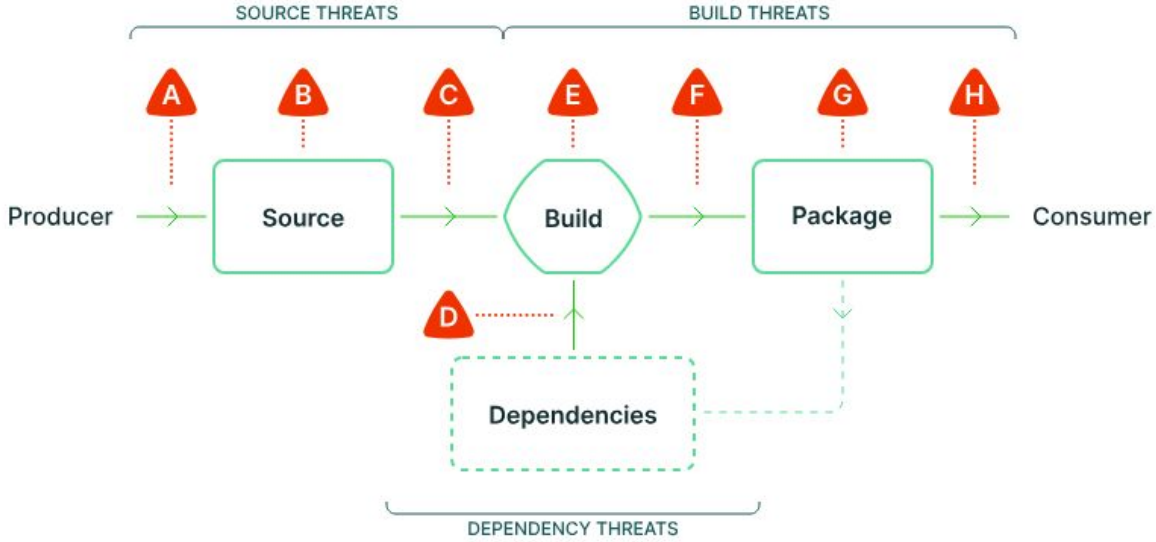
Vulnerability Disclosures
V1. CVD Guides SIGs
V2. OSV Schema project
V3. OpenVEX SIG
OpenVEX Project

Securing Critical Projects
CP1. criticality_score project
CP2. Package Analysis project

ORBIT (Open Resources for Baselines, Interoperability, and Tooling)
O1. OSPS Baseline project

Projects
P1. Alpha & Omega project
P2. Sigstore
P3. Core Toolchain Infrastructure (CTI)

The Supply Chain Problem



SOURCE THREATS

A Submit unauthorized change

B Compromise source repo

C Build from modified source

DEPENDENCY THREATS

D Use compromised dependency

BUILD THREATS

E Compromise build process

F Upload modified package

G Compromise package registry

H Use compromised package

Source: slsa.dev

Ways to Participate

- Join a Working Group/Project
- Come to a Meeting (see Public Calendar)
- Collaborate on Slack
- Contribute on GitHub
- Become an Organizational Member
- Keep up to date by subscribing to the OpenSSF Mailing List

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Engage with us on social media

X
@openssf

LinkedIn
OpenSSF

Mastodon
social.lfx.dev/@openssf

YouTube
OpenSSF

Facebook
OpenSSF

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank You

OpenSSF
OPEN SOURCE SECURITY FOUNDATION