ActiveState

Secure PyPI

How to create a repository of secure Python dependencies

ActiveState

Introductions

Dana Crane

Product Marketing Mgr

Evan Smith

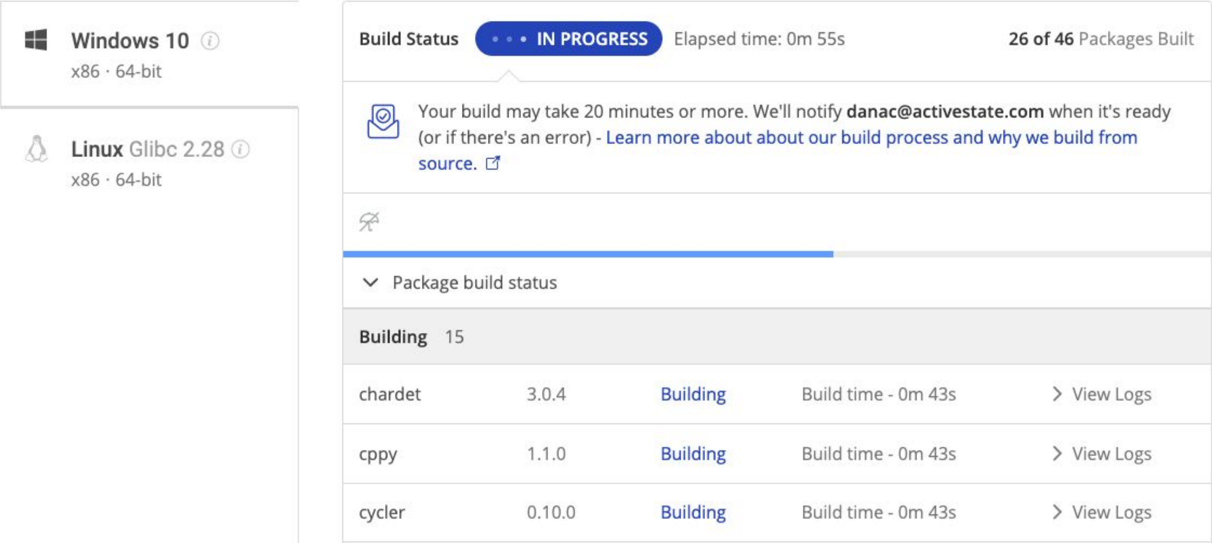
Product Manager

Automating Open Source Language Runtimes

- Automatically build dependencies securely from source code:
  - Eliminate “works on my machine” issues
  - Ensure environment reproducibility
  - Eliminate dependency hell
  - Ensure software supply chain security

Automate Builds from Source

- Automatically build open source from source code + native libraries



Windows 10
x86 · 64-bit

Linux Glibc 2.28
x86 · 64-bit

Build Status • • • IN PROGRESS Elapsed time: 0m 55s **26 of 46** Packages Built

Your build may take 20 minutes or more. We'll notify **danac@activestate.com** when it's ready (or if there's an error) - Learn more about about our build process and why we build from source.

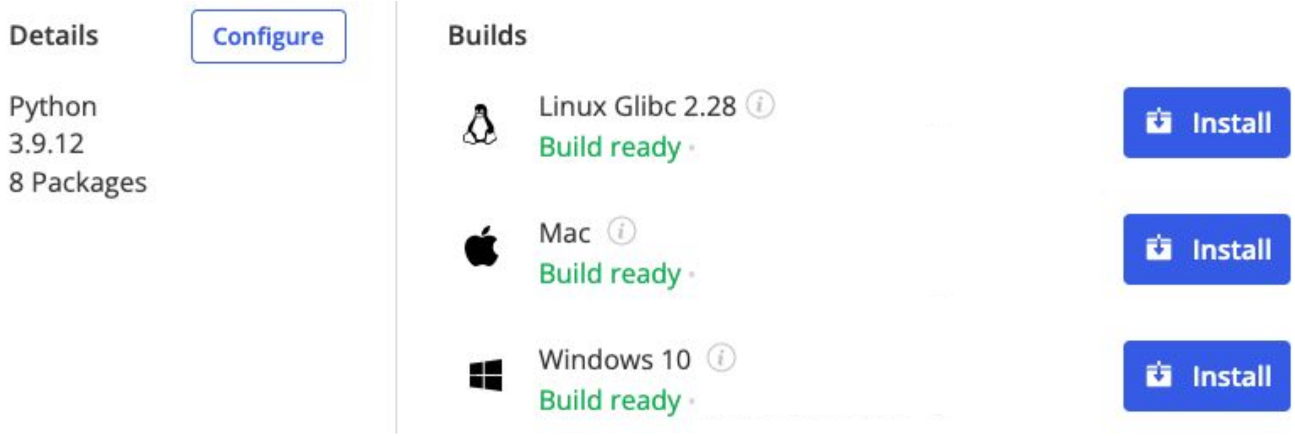
Package build status

Building 15

chardet	3.0.4	Building	Build time - 0m 43s	› View Logs
cppy	1.1.0	Building	Build time - 0m 43s	› View Logs
cycler	0.10.0	Building	Build time - 0m 43s	› View Logs

Shared Runtime Environments

- Eliminate “works on my machine” issues; promotes reproducible environments



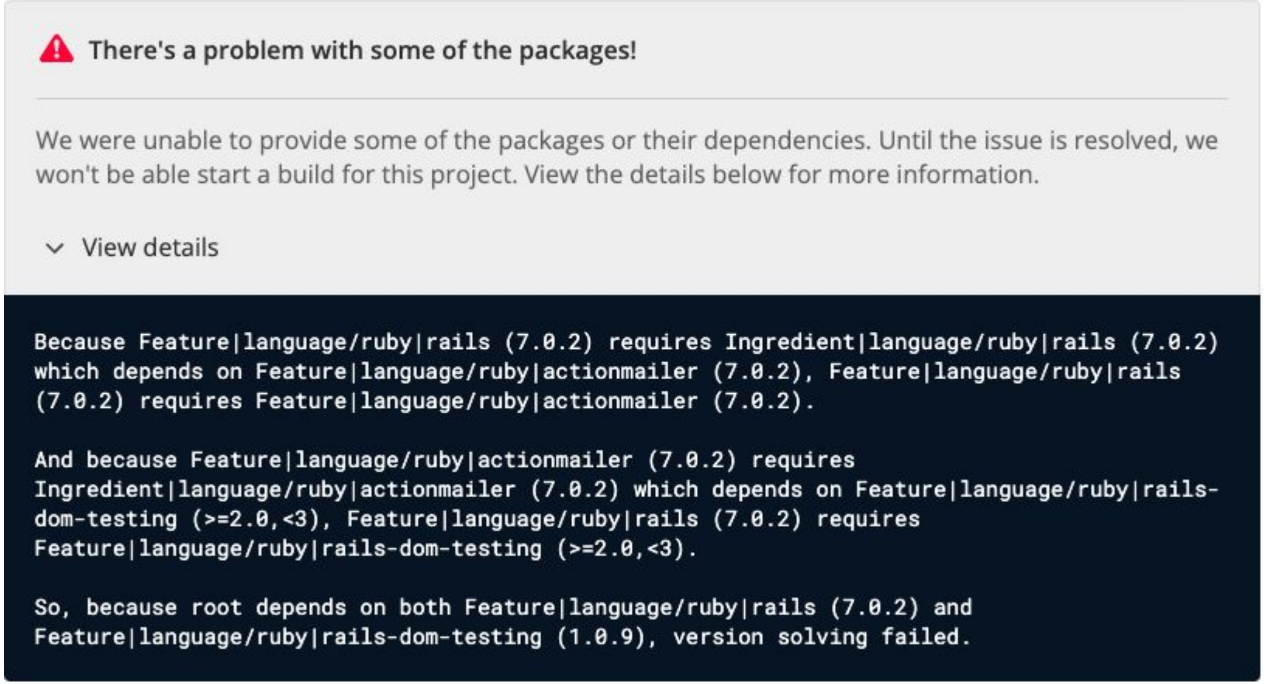
Python
3.9.12
8 Packages

Linux Glibc 2.28
Build ready

Mac
Build ready

Windows 10
Build ready

Eliminate Dependency Hell



⚠ **There's a problem with some of the packages!**

We were unable to provide some of the packages or their dependencies. Until the issue is resolved, we won't be able start a build for this project. View the details below for more information.

```
Because Feature|language/ruby|rails (7.0.2) requires Ingredient|language/ruby|rails (7.0.2)
which depends on Feature|language/ruby|actionmailer (7.0.2), Feature|language/ruby|rails
(7.0.2) requires Feature|language/ruby|actionmailer (7.0.2).

And because Feature|language/ruby|actionmailer (7.0.2) requires
Ingredient|language/ruby|actionmailer (7.0.2) which depends on Feature|language/ruby|rails-
dom-testing (>=2.0,<3), Feature|language/ruby|rails (7.0.2) requires
Feature|language/ruby|rails-dom-testing (>=2.0,<3).

So, because root depends on both Feature|language/ruby|rails (7.0.2) and
Feature|language/ruby|rails-dom-testing (1.0.9), version solving failed.
```

ActiveState

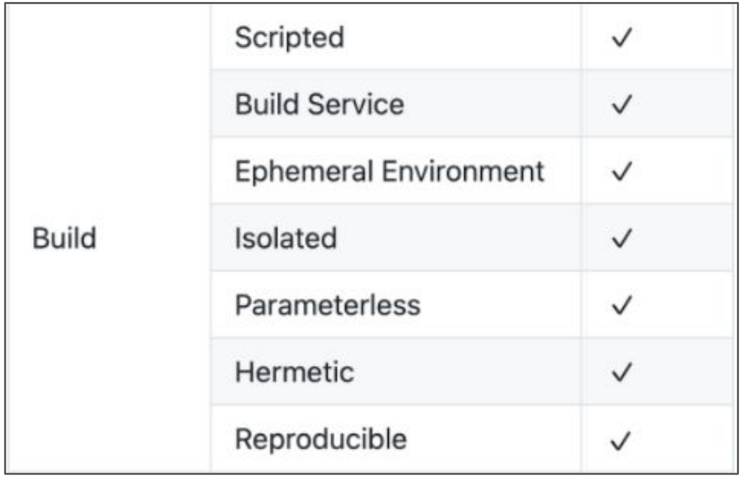
Platform Demo

ActiveState

Secure PyPI

Secure Build Service

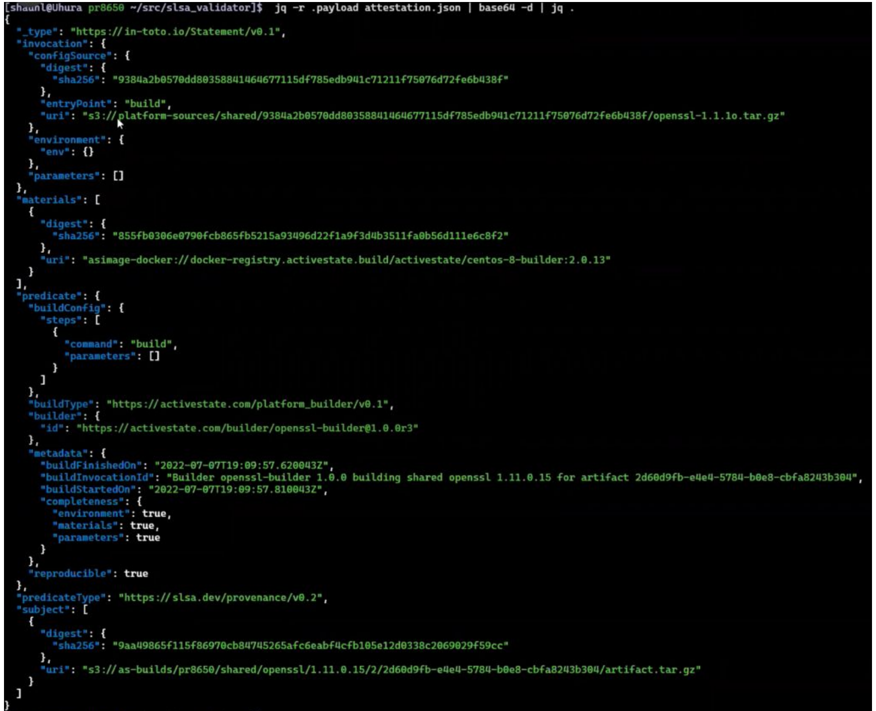
- Tamper-proof system creates reproducible builds of secure artifacts



Build	Scripted	✓
	Build Service	✓
	Ephemeral Environment	✓
	Isolated	✓
	Parameterless	✓
	Hermetic	✓
	Reproducible	✓

Build
SLSA
Source
Deps

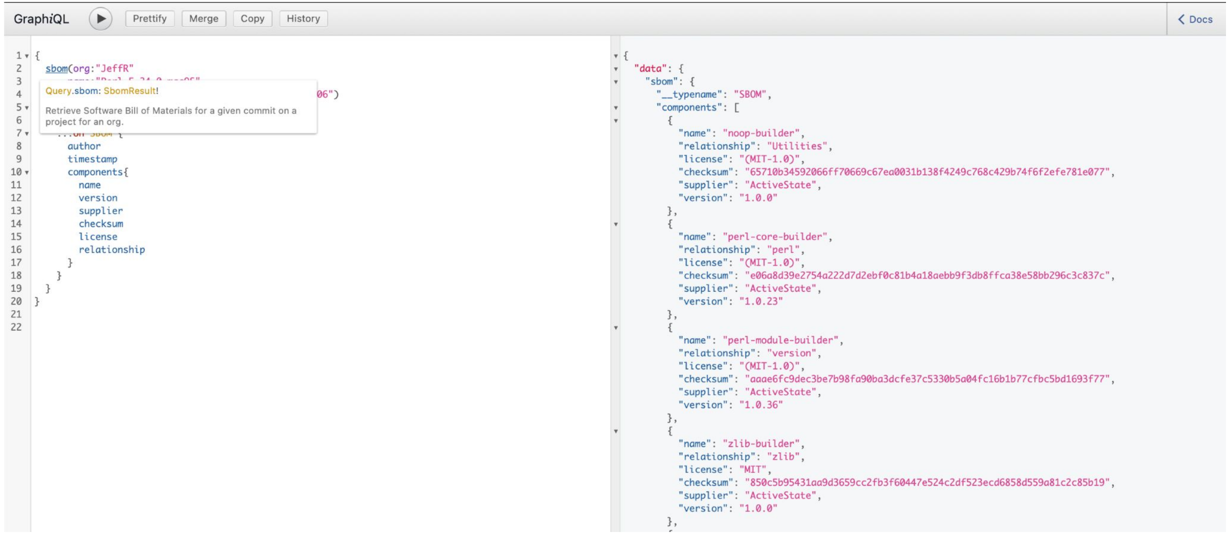
Automatically Generate Attestations



```
[shaunl@Uhura pr8650 ~/src/slsa_validator]$  jq -r .payload attestation.json | base64 -d | jq .
{
  "_type": "https://in-toto.io/Statement/v0.1",
  "invocation": {
    "configSource": {
      "digest": {
        "sha256": "9384a2b0570dd80358841464677115df785edb941c71211f75076d72fe6b438f"
      },
      "entryPoint": "build",
      "uri": "s3://platform-sources/shared/9384a2b0570dd80358841464677115df785edb941c71211f75076d72fe6b438f/openssl-1.1.1o.tar.gz"
    },
    "environment": {
      "env": {}
    },
    "parameters": []
  },
  "materials": [
    {
      "digest": {
        "sha256": "855fb0306e0790fcb865fb5215a93496d22f1a9f3d4b3511fa0b56d111e6c8f2"
      },
      "uri": "asimage-docker://docker-registry.activestate.build/activestate/centos-8-builder:2.0.13"
    }
  ],
  "predicate": {
    "buildConfig": {
      "steps": [
        {
          "command": "build",
          "parameters": []
        }
      ]
    },
    "buildType": "https://activestate.com/platform_builder/v0.1",
    "builder": {
      "id": "https://activestate.com/builder/openssl-builder@1.0.0r3"
    },
    "metadata": {
      "buildFinishedOn": "2022-07-07T19:09:57.620043Z",
      "buildInvocationId": "Builder openssl-builder 1.0.0 building shared openssl 1.11.0.15 for artifact 2d60d9fb-e4e4-5784-b0e8-cbfa8243b304",
      "buildStartedOn": "2022-07-07T19:09:57.810043Z",
      "completeness": {
        "environment": true,
        "materials": true,
        "parameters": true
      }
    },
    "reproducible": true
  },
  "predicateType": "https://slsa.dev/provenance/v0.2",
  "subject": [
    {
      "digest": {
        "sha256": "9aa49865f115f86970cb84745265afc6eabf4cfb105e12d0338c2069029f59cc"
      },
      "uri": "s3://as-builds/pr8650/shared/openssl/1.11.0.15/2/2d60d9fb-e4e4-5784-b0e8-cbfa8243b304/artifact.tar.gz"
    }
  ]
}
```

Automatically Generate SBOMs

- Software Bill Of Materials (SBOM) for each of your runtime environments



```
{
  sbom(org:"JeffR"
      name:"Perl-5.24.0-macOS"
                                                06")


    ...on SBOM {
      author
      timestamp
      components{
        name
        version
        supplier
        checksum
        license
        relationship
      }
    }
  }
}
```

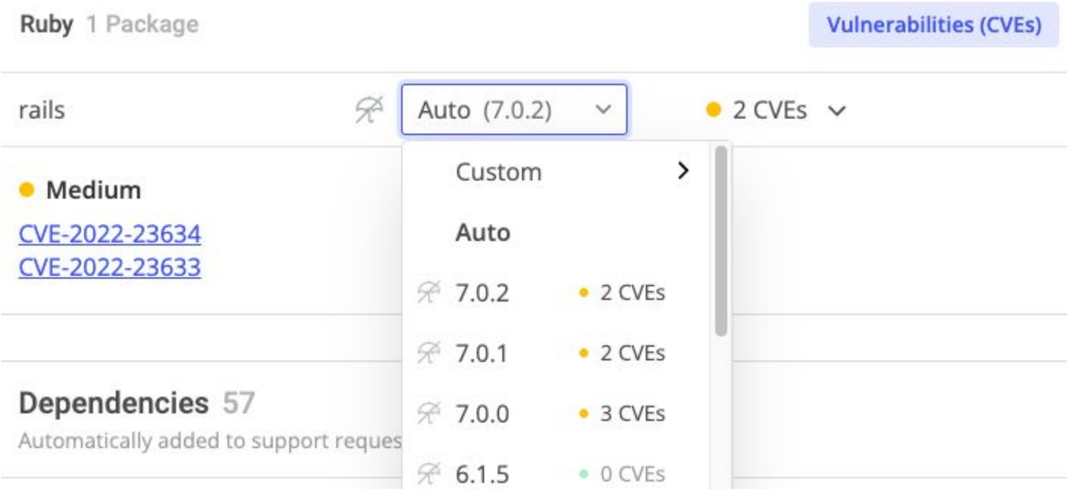
Query.sbom: SbomResult!

Retrieve Software Bill of Materials for a given commit on a project for an org.

```
{
  "data": {
    "sbom": {
      "__typename": "SBOM",
      "components": [
        {
          "name": "noop-builder",
          "relationship": "Utilities",
          "license": "(MIT-1.0)",
          "checksum": "65710b34592066ff70669c67ea0031b138f4249c768c429b74f6f2efe781e077",
          "supplier": "ActiveState",
          "version": "1.0.0"
        },
        {
          "name": "perl-core-builder",
          "relationship": "perl",
          "license": "(MIT-1.0)",
          "checksum": "e06a8d39e2754a222d7d2ebf0c81b4a18aebb9f3db8ffca38e58bb296c3c837c",
          "supplier": "ActiveState",
          "version": "1.0.23"
        },
        {
          "name": "perl-module-builder",
          "relationship": "version",
          "license": "(MIT-1.0)",
          "checksum": "aaae6fc9dec3be7b98fa90ba3dcfe37c5330b5a04fc16b1b77cfbc5bd1693f77",
          "supplier": "ActiveState",
          "version": "1.0.36"
        },
        {
          "name": "zlib-builder",
          "relationship": "zlib",
          "license": "MIT",
          "checksum": "850c5b95431aa9d3659cc2fb3f60447e524c2df523ecd6858d559a81c2c85b19",
          "supplier": "ActiveState",
          "version": "1.0.0"
        },
        {
```

Automate Vulnerability Management

- Automatically monitor, notify and simplify remediation of vulnerabilities



Ruby 1 Package

Vulnerabilities (CVEs)

rails Auto (7.0.2) ● 2 CVEs

● Medium

CVE-2022-23634
CVE-2022-23633

Dependencies 57

Automatically added to support reques

Distribute Secure Python Packages

ActiveState Platform vs Artifact Repository

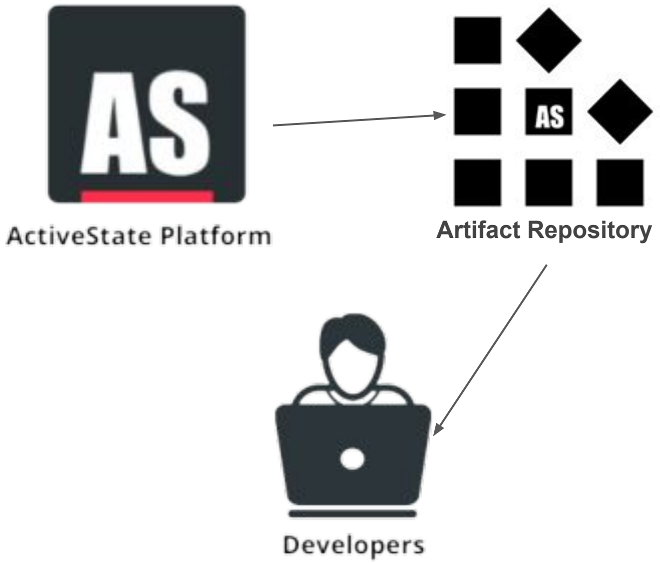
ActiveState Platform:

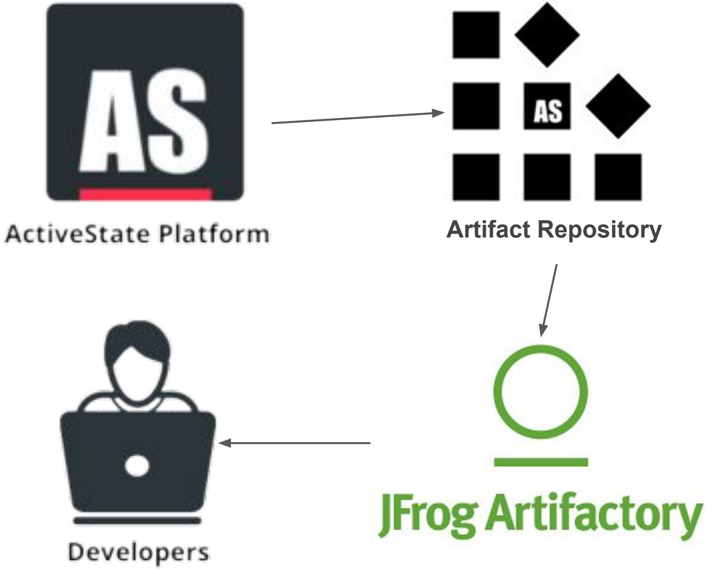
- Does not support pip installs
- Includes Python and OS dependencies

Artifact Repository:

- Support pip installs
- Does not include Python or OS dependencies

Python Dependency Distribution





Why ActiveState Artifact Repository?

- **Enable Supply Chain Security** - ensure data scientists and developers can work securely from sandbox to production.
- **Create a Curated Catalog** - ensure all coders work only with approved Python dependencies.
- **Standardize Extensibility** - install a standard Python deployment backed by an approved set of packages from the ActiveState Artifact Repository.
- **Eliminate Retraining** - instead of learning the State Tool, developers and data scientists can continue working with the tools (like pip) that they already know

ActiveState

Artifact Repository Demo

ActiveState

Q&A

ActiveState

Next Steps

Schedule a demo with our product experts:
https://www.activestate.com/get-demo/

Learn more about ActiveState Artifact Repository:
https://www.activestate.com/solutions/artifact-repository/

Try the ActiveState Platform for free:
https://platform.activestate.com/