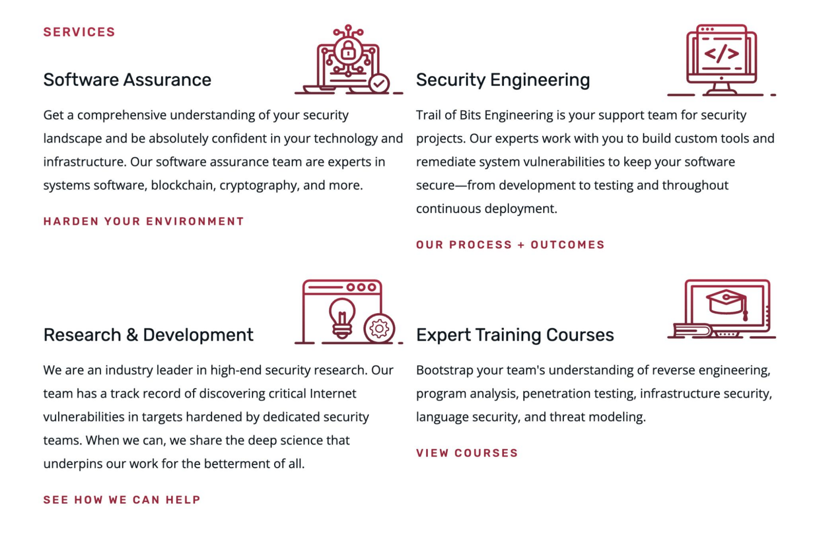
TRAIL OF BITS

Build Provenance: Lessons (so Far) from Homebrew

Who am I?

Joe Sweeney - Security Engineer - Trail of Bits



SERVICES

Software Assurance

Get a comprehensive understanding of your security landscape and be absolutely confident in your technology and infrastructure. Our software assurance team are experts in systems software, blockchain, cryptography, and more.

HARDEN YOUR ENVIRONMENT

Security Engineering

Trail of Bits Engineering is your support team for security projects. Our experts work with you to build custom tools and remediate system vulnerabilities to keep your software secure—from development to testing and throughout continuous deployment.

OUR PROCESS + OUTCOMES

Research & Development

We are an industry leader in high-end security research. Our team has a track record of discovering critical Internet vulnerabilities in targets hardened by dedicated security teams. When we can, we share the deep science that underpins our work for the betterment of all.

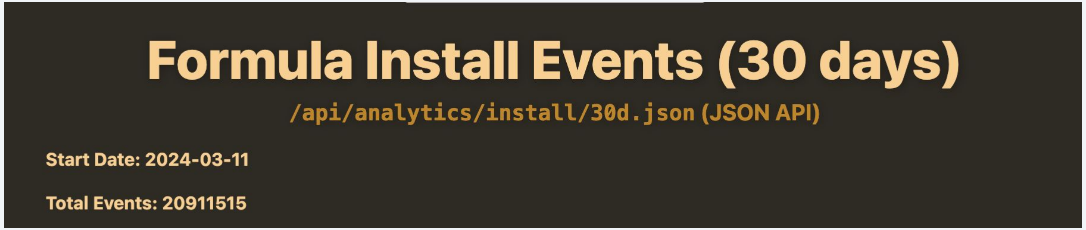
SEE HOW WE CAN HELP

Expert Training Courses

Bootstrap your team's understanding of reverse engineering, program analysis, penetration testing, infrastructure security, language security, and threat modeling.

VIEW COURSES

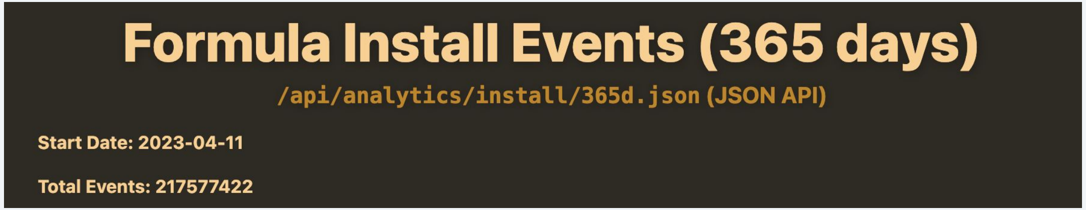
What is Homebrew? Why does it need build provenance?


Formula Install Events (30 days)

`/api/analytics/install/30d.json` (JSON API)

Start Date: 2024-03-11

Total Events: 20911515

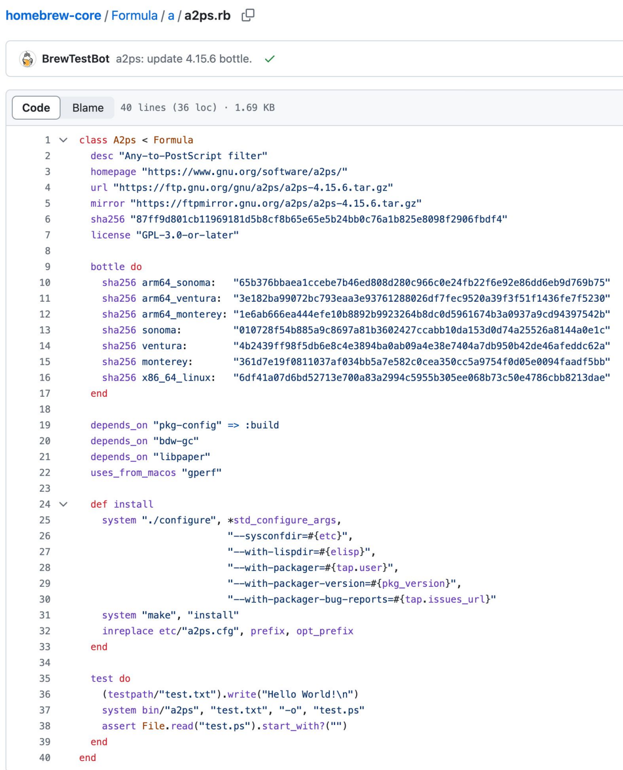

Formula Install Events (365 days)

`/api/analytics/install/365d.json` (JSON API)

Start Date: 2023-04-11

Total Events: 217577422

Formula? Bottles?



homebrew-core / Formula / a / a2ps.rb

BrewTestBot a2ps: update 4.15.6 bottle. ✓

40 lines (36 loc) · 1.69 KB

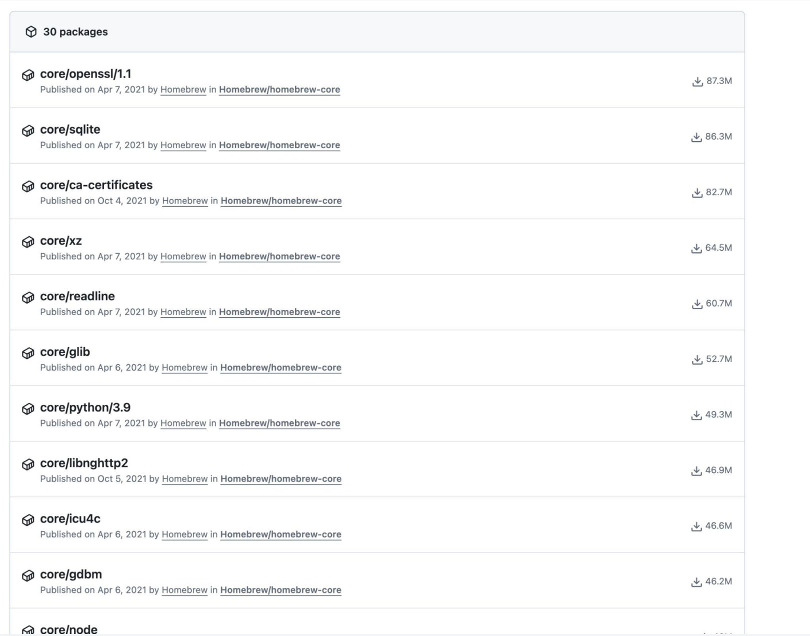
```ruby
class A2ps < Formula
  desc "Any-to-PostScript filter"
  homepage "https://www.gnu.org/software/a2ps/"
  url "https://ftp.gnu.org/gnu/a2ps/a2ps-4.15.6.tar.gz"
  mirror "https://ftpmirror.gnu.org/a2ps/a2ps-4.15.6.tar.gz"
  sha256 "87ff9d801cb11969181d5b8cf8b65e65e5b24bb0c76a1b825e8098f2906fbdf4"
  license "GPL-3.0-or-later"

  bottle do
    sha256 arm64_sonoma:   "65b376bbaea1ccebe7b46ed808d280c966c0e24fb22f6e92e86dd6eb9d769b75"
    sha256 arm64_ventura:  "3e182ba99072bc793eaa3e93761288026df7fec9520a39f3f51f1436fe7f5230"
    sha256 arm64_monterey: "1e6ab666ea444efe10b8892b9923264b8dc0d5961674b3a0937a9cd94397542b"
    sha256 sonoma:         "010728f54b885a9c8697a81b3602427ccabb10da153d0d74a25526a8144a0e1c"
    sha256 ventura:        "4b2439ff98f5db6e8c4e3894ba0ab09a4e38e7404a7db950b42de46afeddc62a"
    sha256 monterey:       "361d7e19f0811037af034bb5a7e582c0cea350cc5a9754f0d05e0094faadf5bb"
    sha256 x86_64_linux:   "6df41a07d6bd52713e700a83a2994c5955b305ee068b73c50e4786cbb8213dae"
  end

  depends_on "pkg-config" => :build
  depends_on "bdw-gc"
  depends_on "libpaper"
  uses_from_macos "gperf"

  def install
    system "./configure", *std_configure_args,
                          "--sysconfdir=#{etc}",
                          "--with-lispdir=#{elisp}",
                          "--with-packager=#{tap.user}",
                          "--with-packager-version=#{pkg_version}",
                          "--with-packager-bug-reports=#{tap.issues_url}"
    system "make", "install"
    inreplace etc/"a2ps.cfg", prefix, opt_prefix
  end

  test do
    (testpath/"test.txt").write("Hello World!\n")
    system bin/"a2ps", "test.txt", "-o", "test.ps"
    assert File.read("test.ps").start_with?("")
  end
end
```



30 packages

core/openssl/1.1
Published on Apr 7, 2021 by Homebrew in Homebrew/homebrew-core — 87.3M

core/sqlite
Published on Apr 7, 2021 by Homebrew in Homebrew/homebrew-core — 86.3M

core/ca-certificates
Published on Oct 4, 2021 by Homebrew in Homebrew/homebrew-core — 82.7M

core/xz
Published on Apr 7, 2021 by Homebrew in Homebrew/homebrew-core — 64.5M

core/readline
Published on Apr 7, 2021 by Homebrew in Homebrew/homebrew-core — 60.7M

core/glib
Published on Apr 6, 2021 by Homebrew in Homebrew/homebrew-core — 52.7M

core/python/3.9
Published on Apr 7, 2021 by Homebrew in Homebrew/homebrew-core — 49.3M

core/libnghttp2
Published on Oct 5, 2021 by Homebrew in Homebrew/homebrew-core — 46.9M

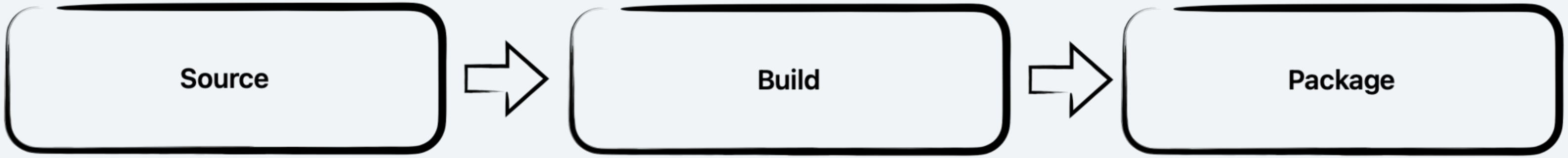
core/icu4c
Published on Apr 6, 2021 by Homebrew in Homebrew/homebrew-core — 46.6M

core/gdbm
Published on Apr 6, 2021 by Homebrew in Homebrew/homebrew-core — 46.2M

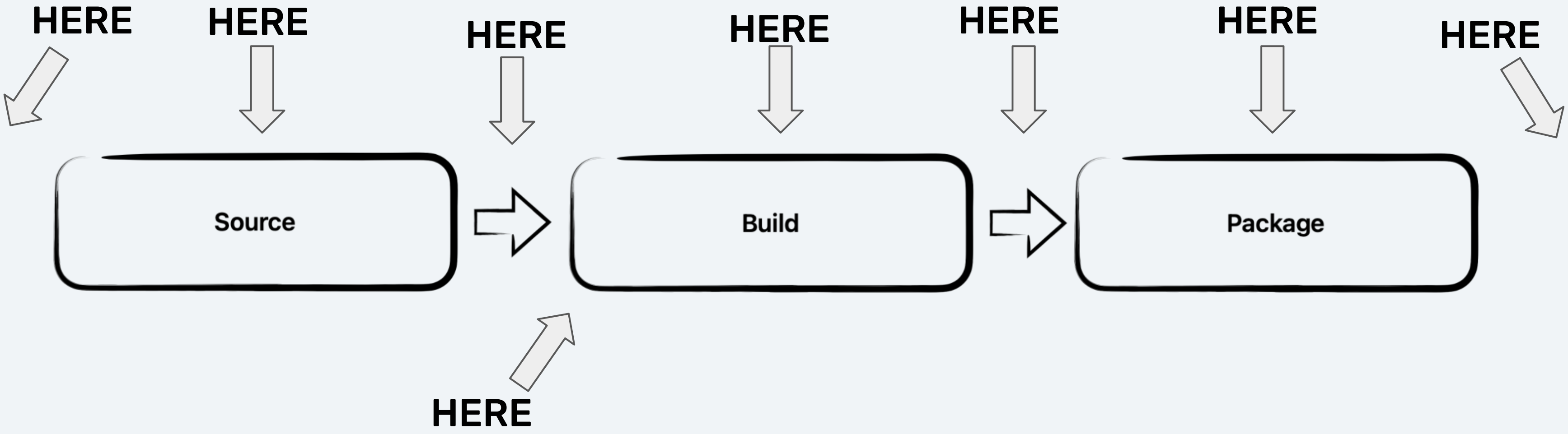
core/node

https://github.com/orgs/Homebrew/packages

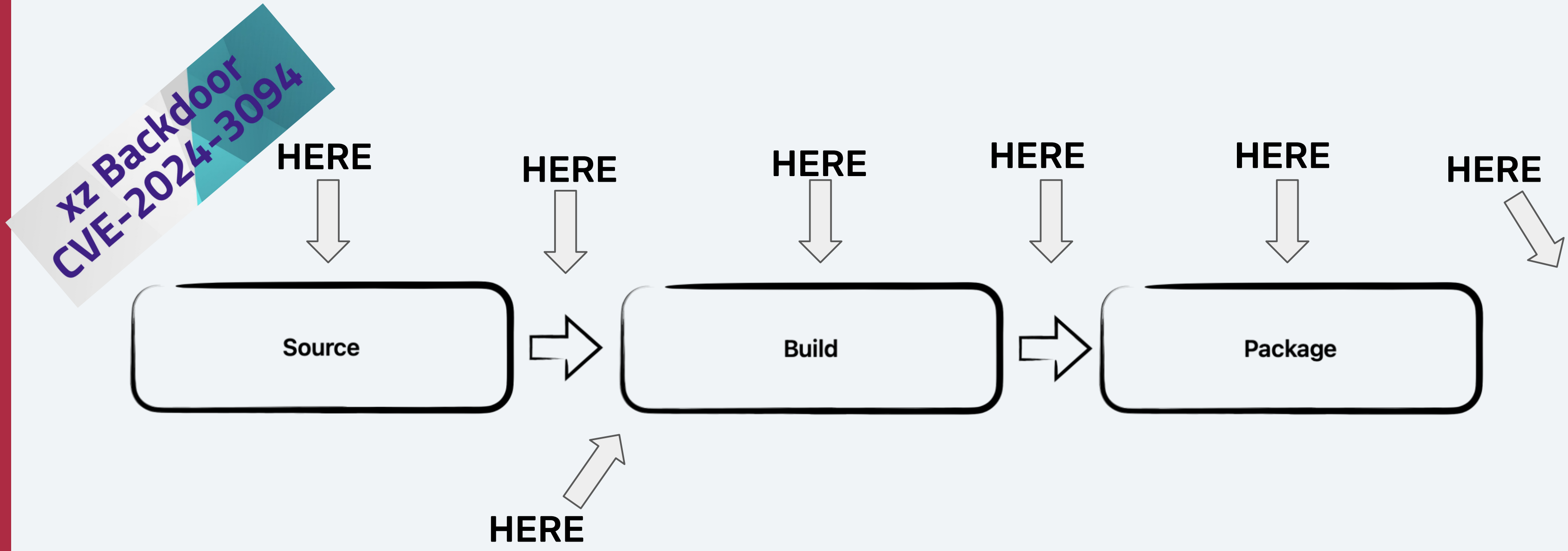
What is build provenance?



What is build provenance?



What is build provenance?



xz Backdoor
CVE-2024-3094

HERE

HERE

HERE

HERE

HERE

HERE

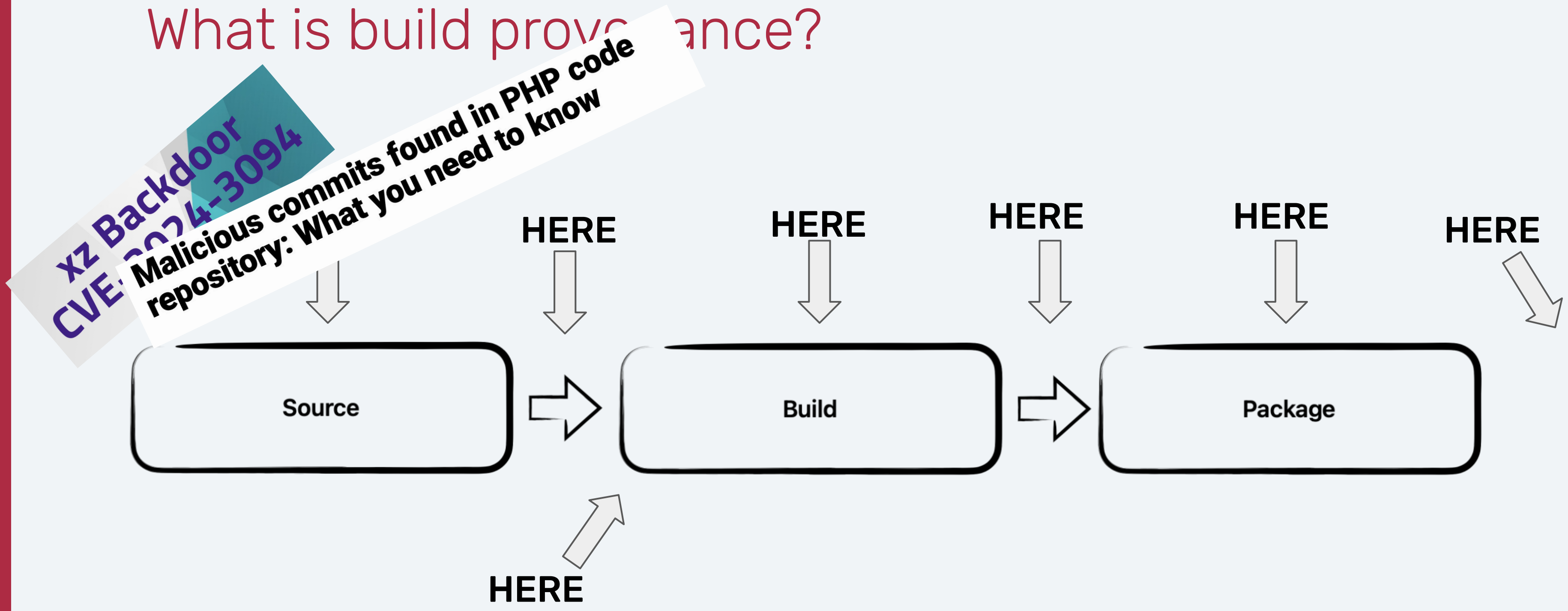
Source

Build

Package

HERE

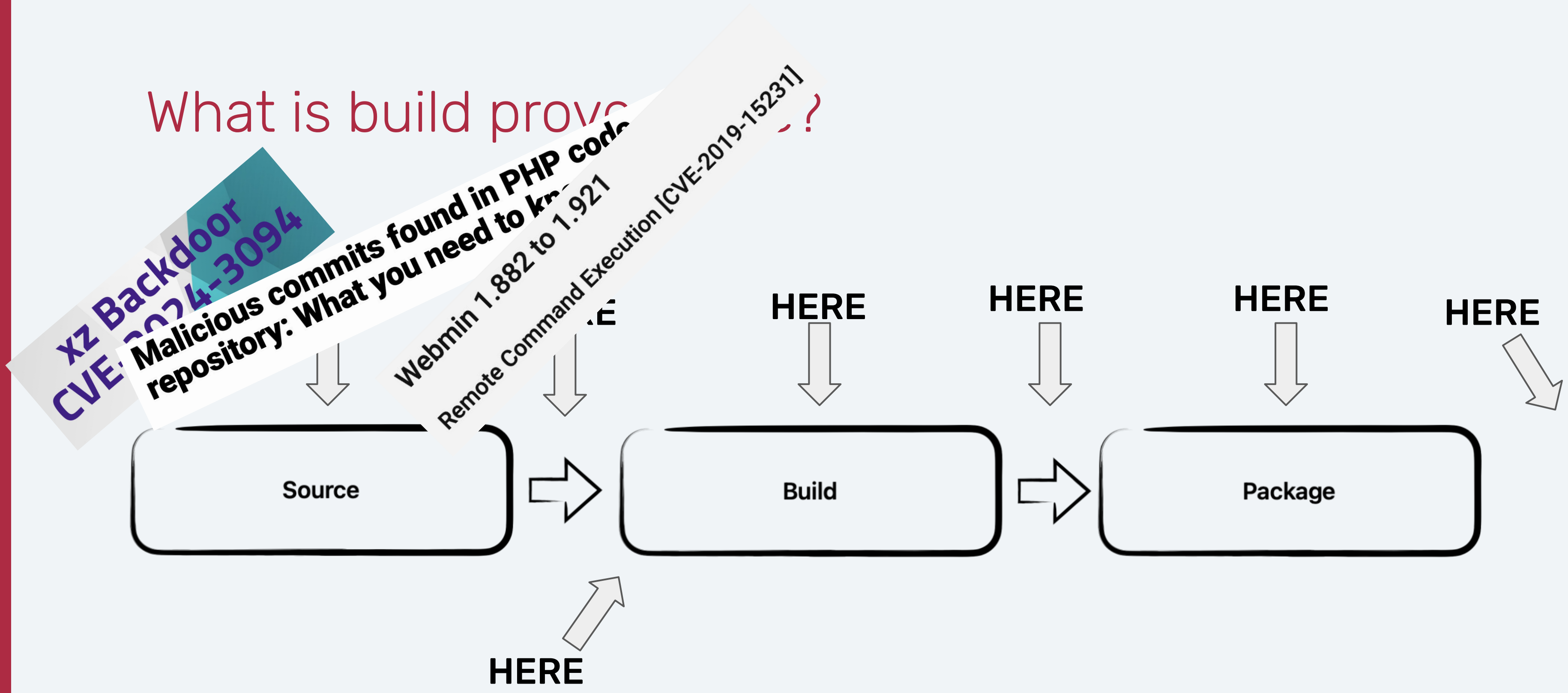
What is build provenance?



xz Backdoor
CVE-2024-3094

Malicious commits found in PHP code repository: What you need to know

What is build prov ?

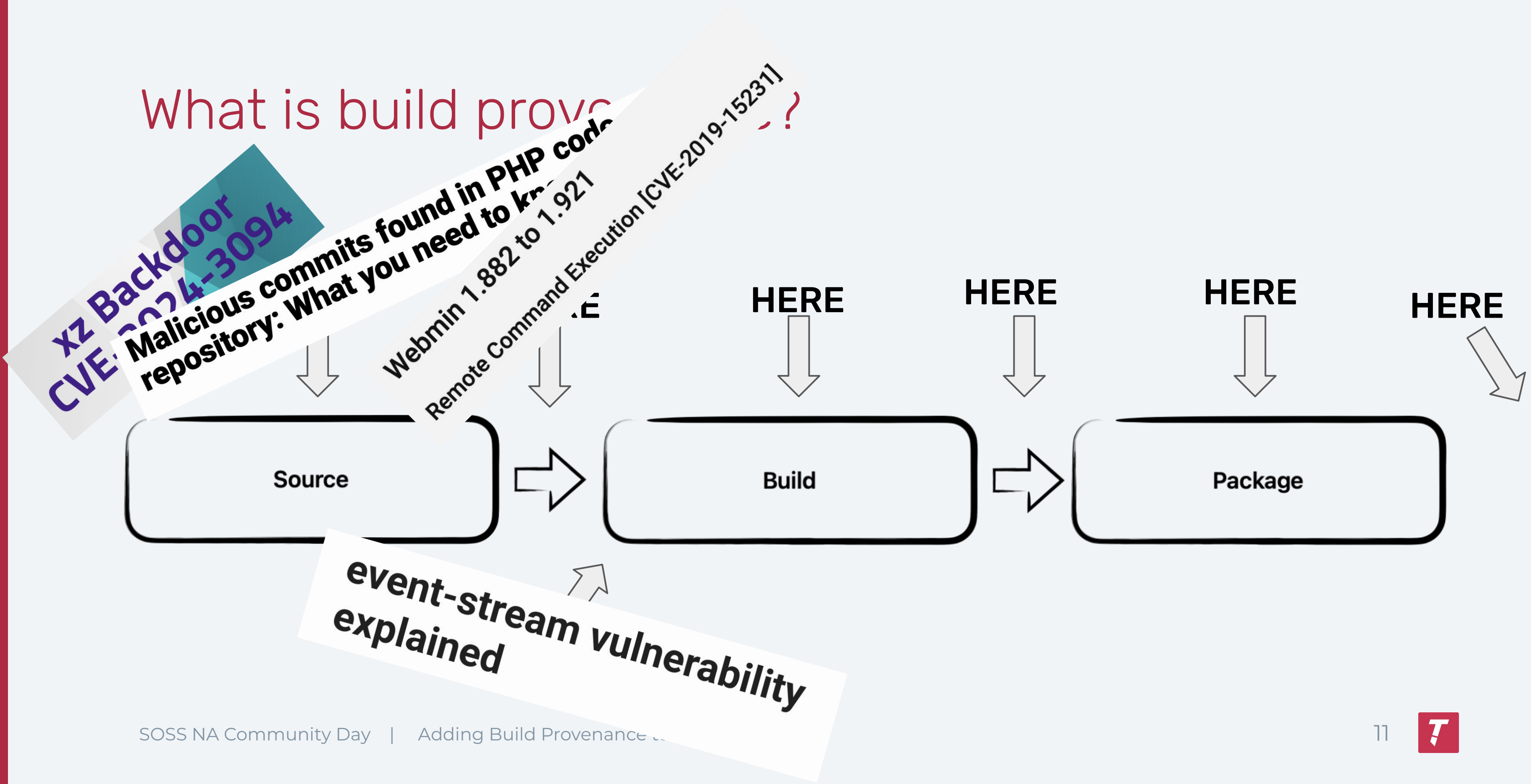


xz Backdoor
CVE-2024-3094

Malicious commits found in PHP code repository: What you need to kn

Webmin 1.882 to 1.921
Remote Command Execution [CVE-2019-15231]

What is build prov?



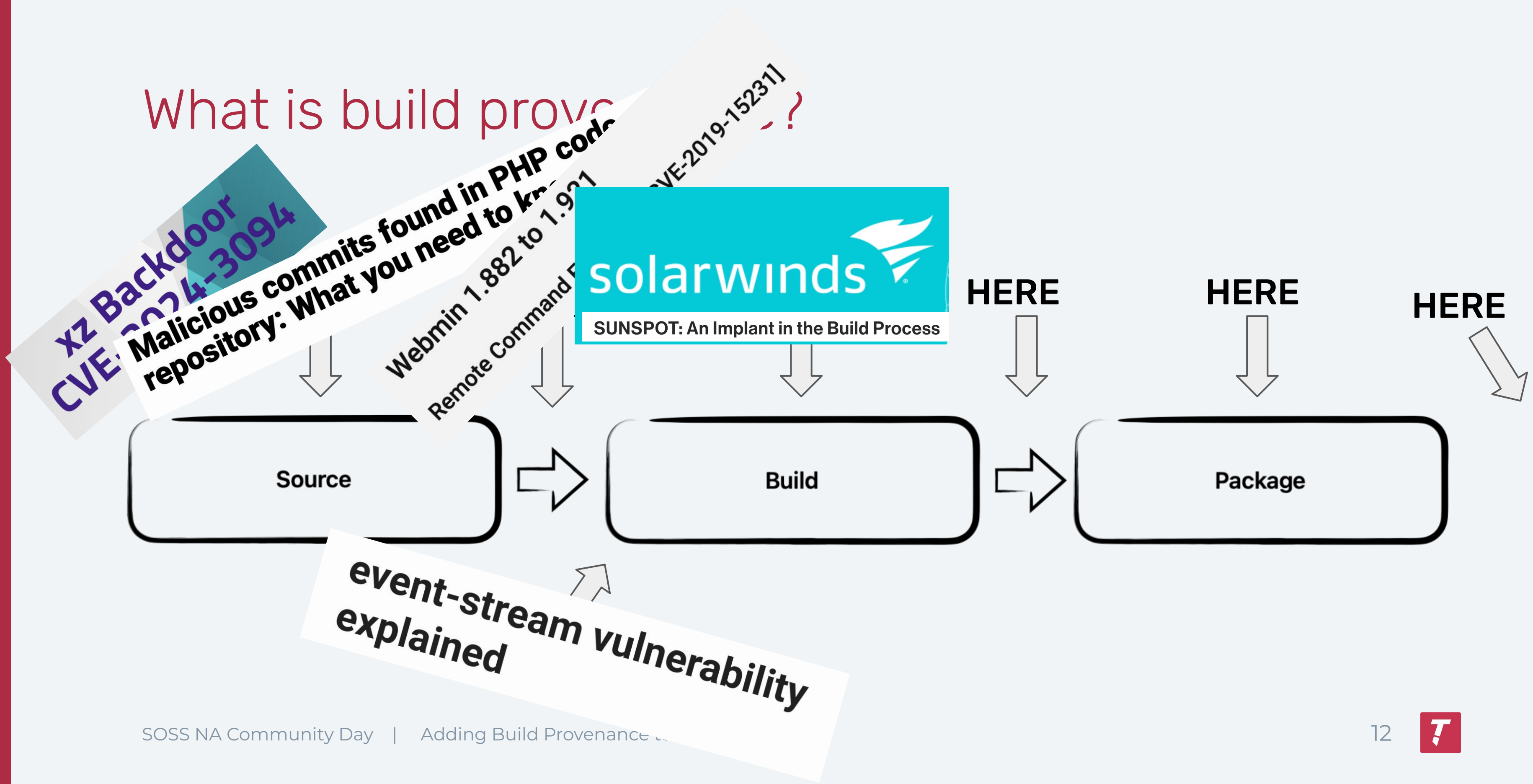
xz Backdoor
CVE-2024-3094

Malicious commits found in PHP code repository: What you need to kn

Webmin 1.882 to 1.921
Remote Command Execution [CVE-2019-15231]

event-stream vulnerability explained

What is build prov ?



xz Backdoor
CVE-2024-3094

Malicious commits found in PHP code repository: What you need to kn

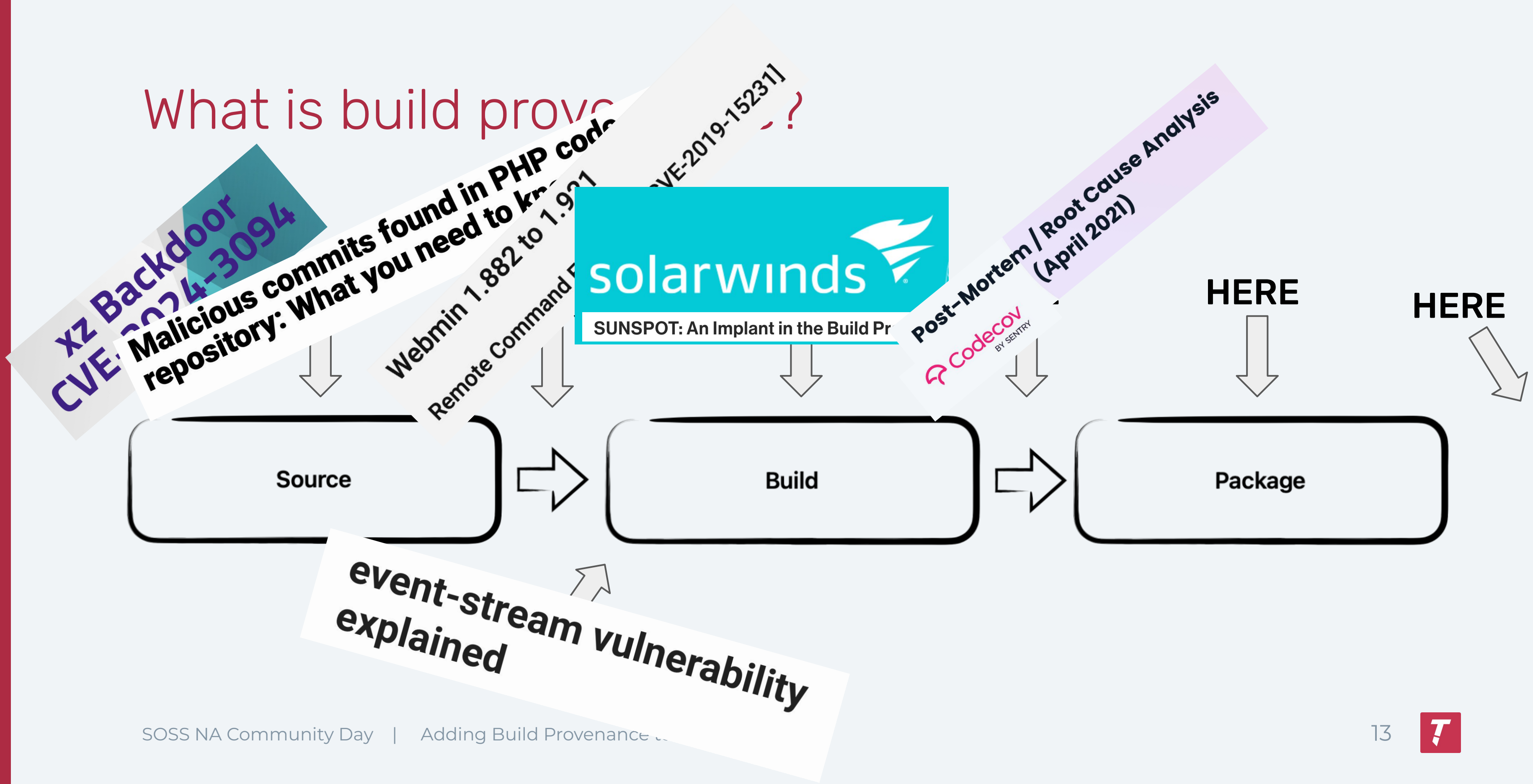
Webmin 1.882 to 1.921 - Remote Command E [CVE-2019-15231]

solarwinds

SUNSPOT: An Implant in the Build Process

event-stream vulnerability explained

What is build prov ?



xz Backdoor CVE-2024-3094

Malicious commits found in PHP code repository: What you need to kn

Webmin 1.882 to 1.921 Remote Command E

VE-2019-15231]

solarwinds

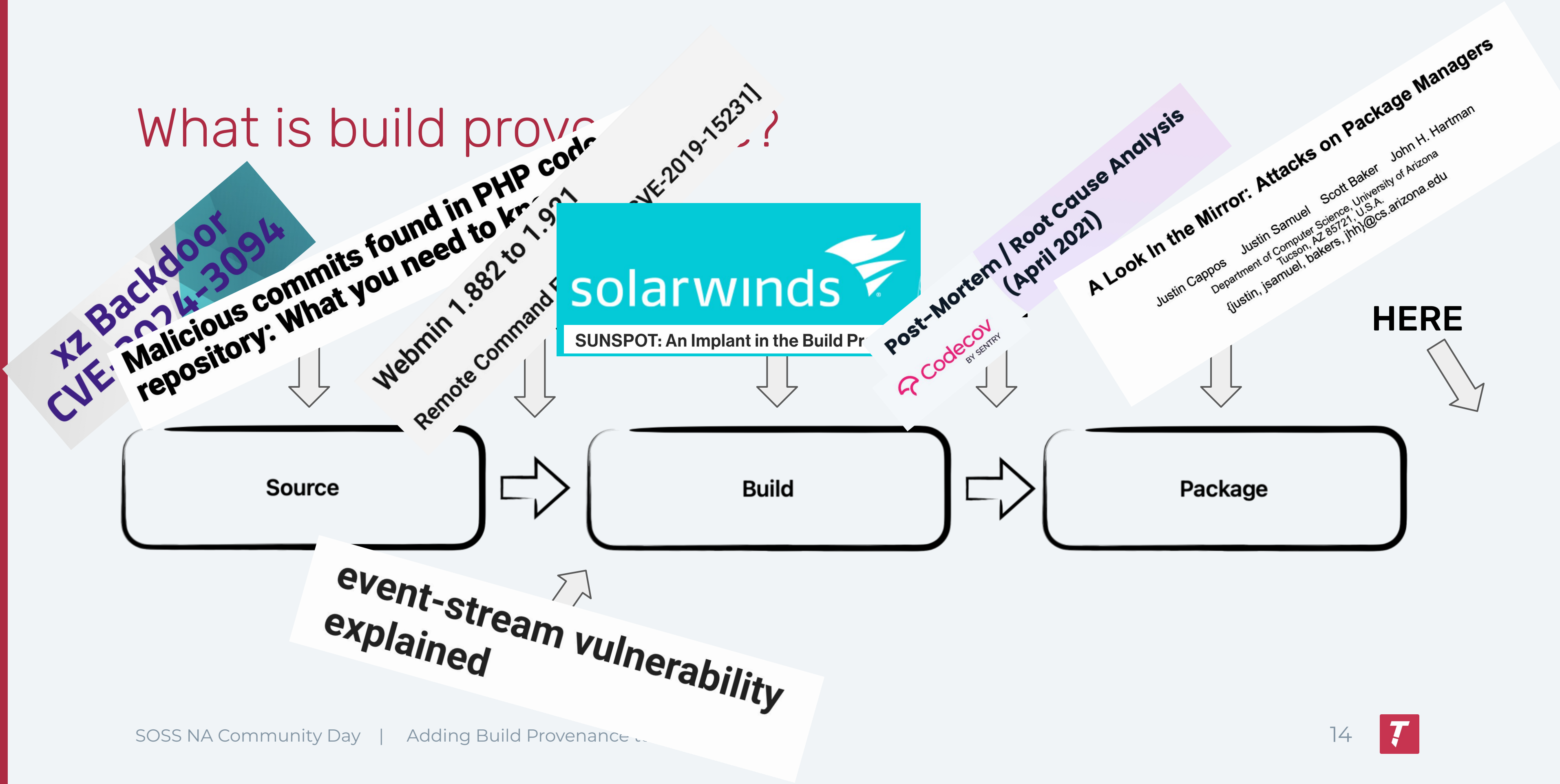
SUNSPOT: An Implant in the Build Pr

Post-Mortem / Root Cause Analysis (April 2021)

Codecov BY SENTRY

event-stream vulnerability explained

What is build prov ?



xz Backdoor
CVE-2024-3094

Malicious commits found in PHP code repository: What you need to kn

Webmin 1.882 to 1.921 Remote Command E [CVE-2019-15231]

SUNSPOT: An Implant in the Build Pr

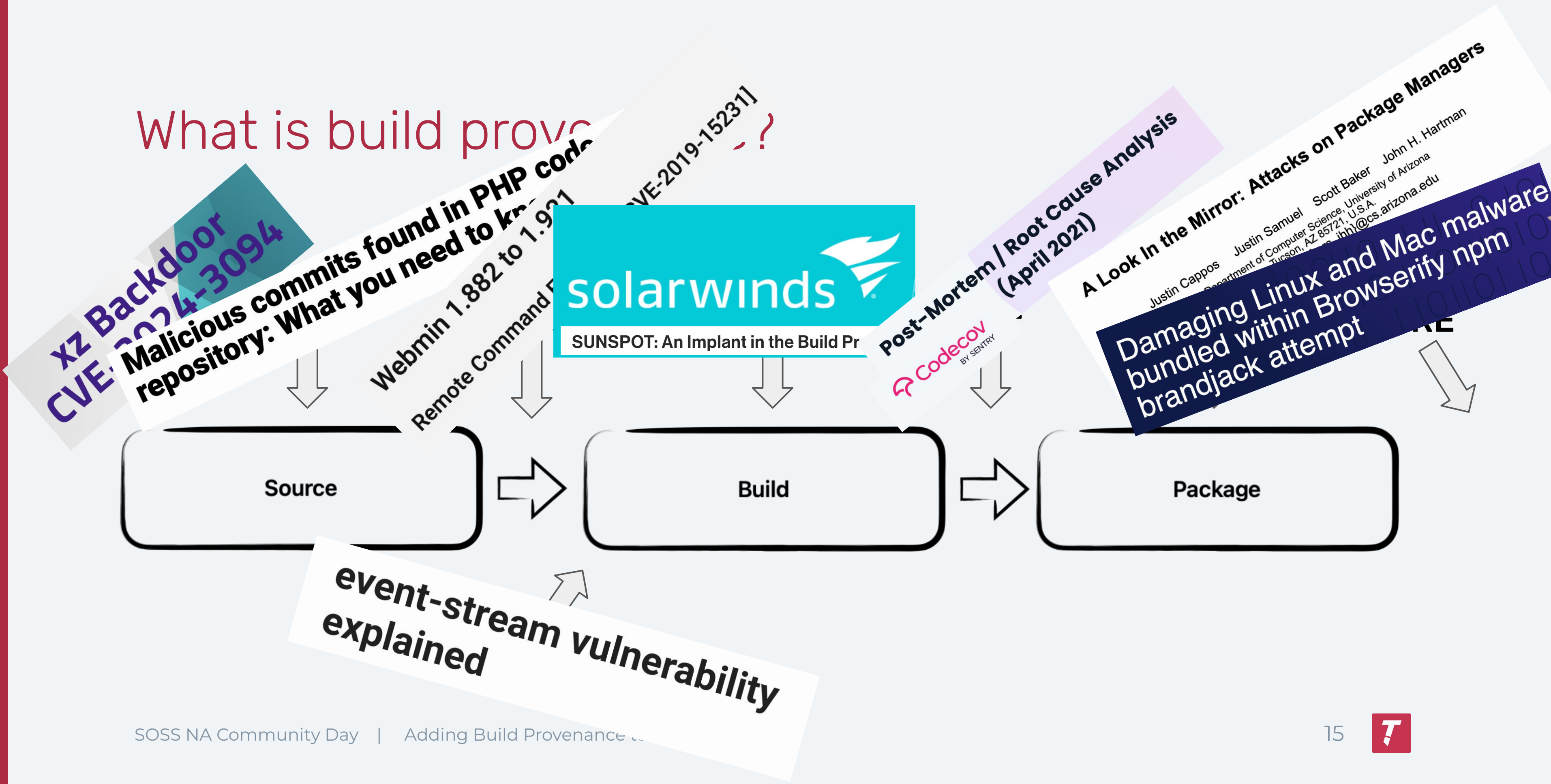
Post-Mortem / Root Cause Analysis (April 2021)

A Look In the Mirror: Attacks on Package Managers

Justin Cappos Justin Samuel Scott Baker John H. Hartman
Department of Computer Science, University of Arizona
Tucson, AZ 85721, U.S.A.
{justin, jsamuel, bakers, jhh}@cs.arizona.edu

event-stream vulnerability explained

What is build prov ?



xz Backdoor
CVE-2024-3094

Malicious commits found in PHP code repository: What you need to kn

Webmin 1.882 to 1.921 Remote Command E [CVE-2019-15231]

solarwinds

SUNSPOT: An Implant in the Build Pr

Post-Mortem / Root Cause Analysis (April 2021)

codecov BY SENTRY

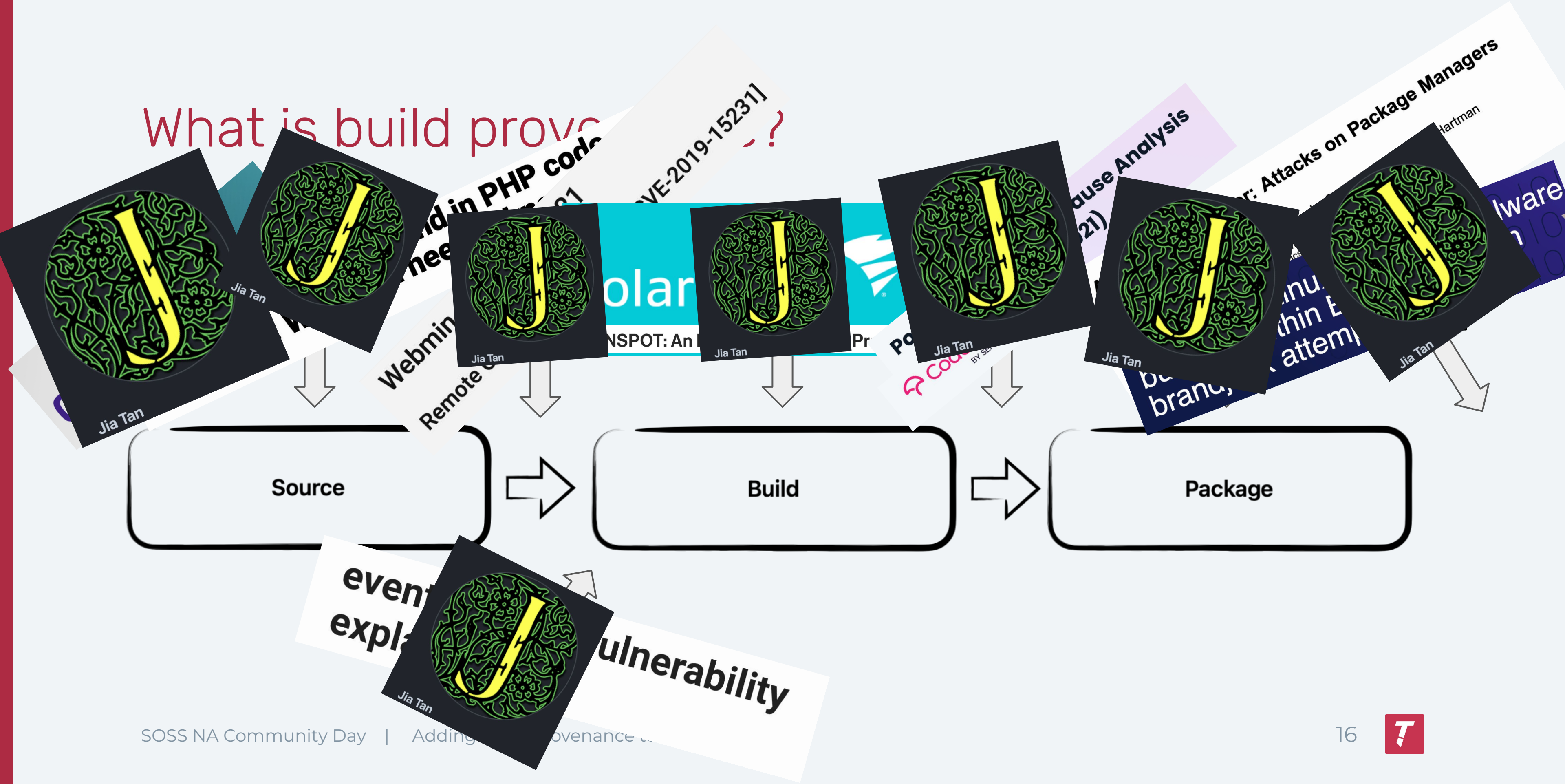
A Look In the Mirror: Attacks on Package Managers

Justin Cappos Justin Samuel Scott Baker John H. Hartman
Department of Computer Science, University of Arizona
Tucson, AZ 85721, U.S.A.
jhh}@cs.arizona.edu

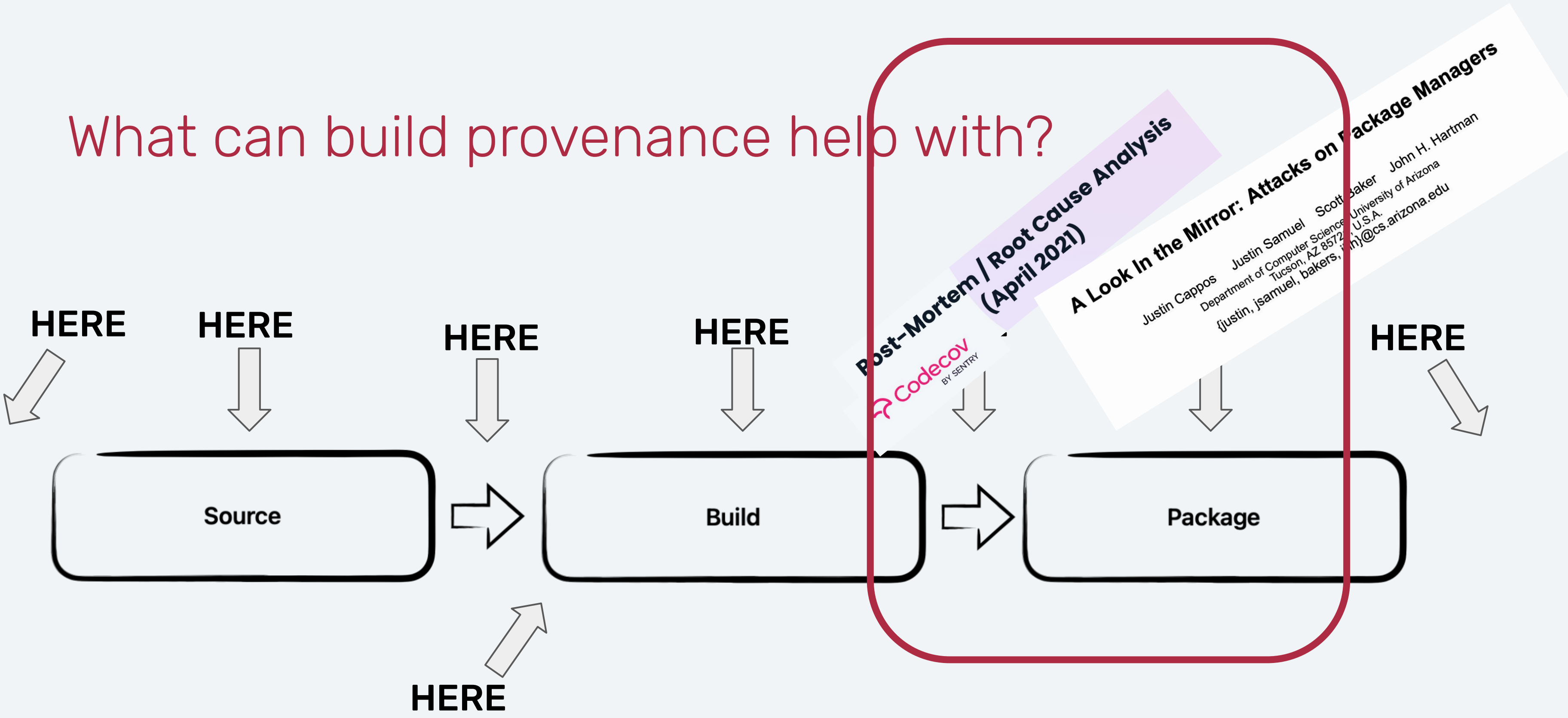
Damaging Linux and Mac malware bundled within Browserify npm brandjack attempt

event-stream vulnerability explained

What is build prov ?



What can build provenance help with?



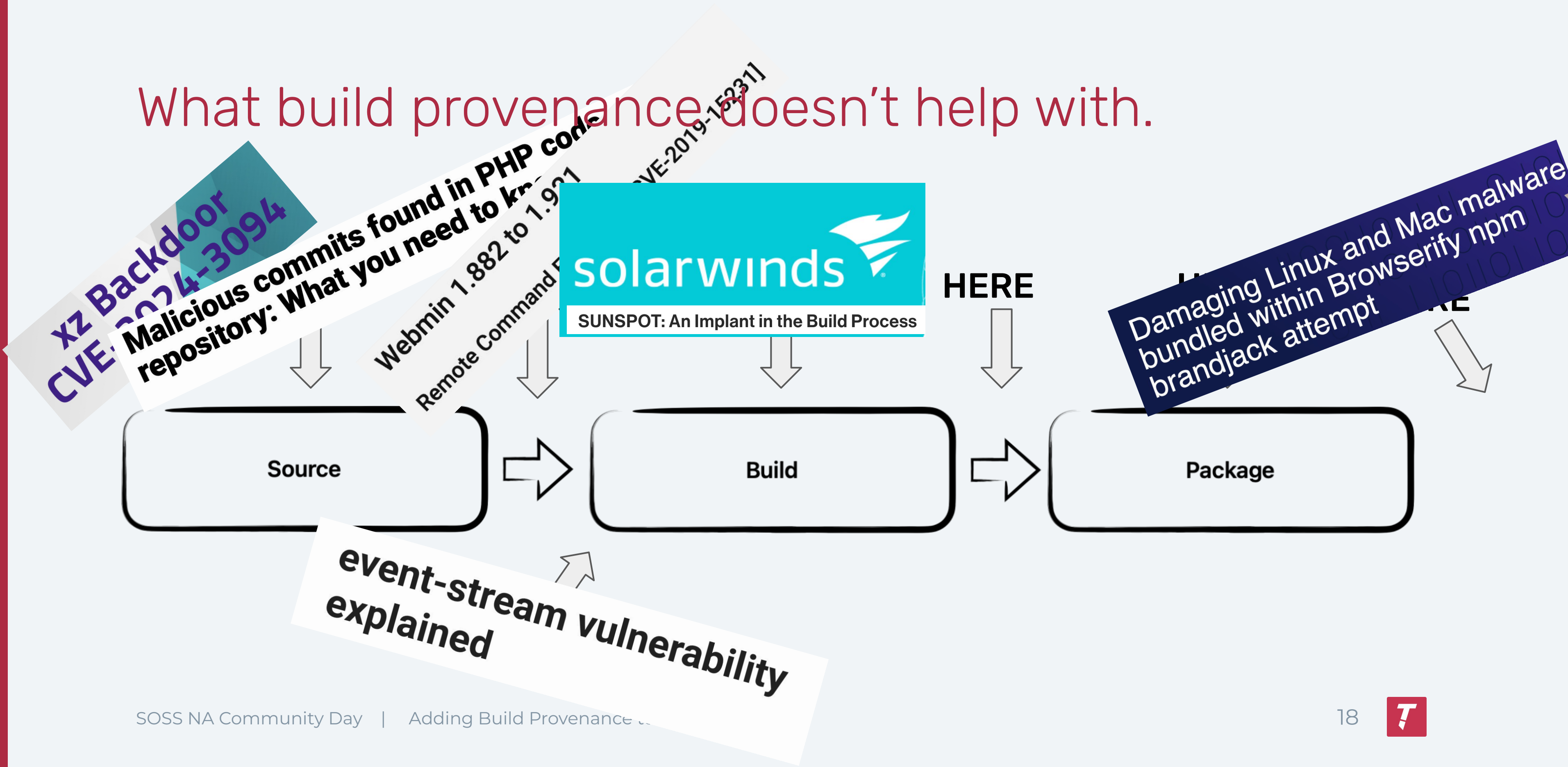
Post-Mortem / Root Cause Analysis (April 2021)

Codecov BY SENTRY

A Look In the Mirror: Attacks on Package Managers

Justin Cappos Justin Samuel Scott Baker John H. Hartman
Department of Computer Science, University of Arizona
Tucson, AZ 85721, U.S.A.
{justin, jsamuel, bakers, jhh}@cs.arizona.edu

What build provenance doesn’t help with.



xz Backdoor
CVE-2024-3094

Malicious commits found in PHP cod
repository: What you need to kn

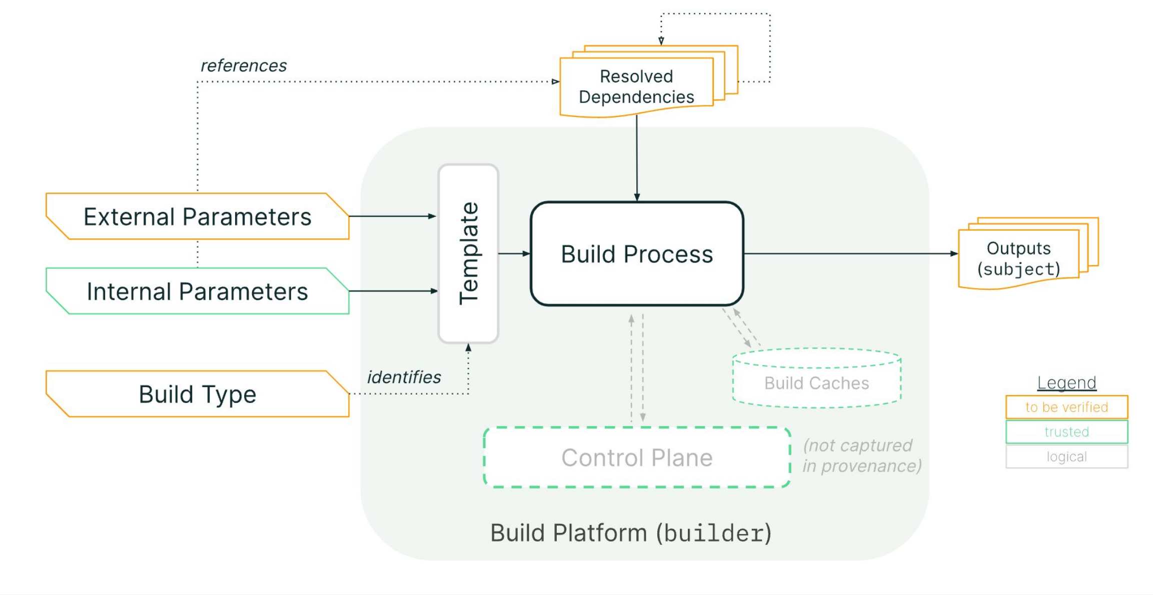
Webmin 1.882 to 1.921
Remote Command E
VE-2019-15231]

SUNSPOT: An Implant in the Build Process

Damaging Linux and Mac malware bundled within Browserify npm brandjack attempt

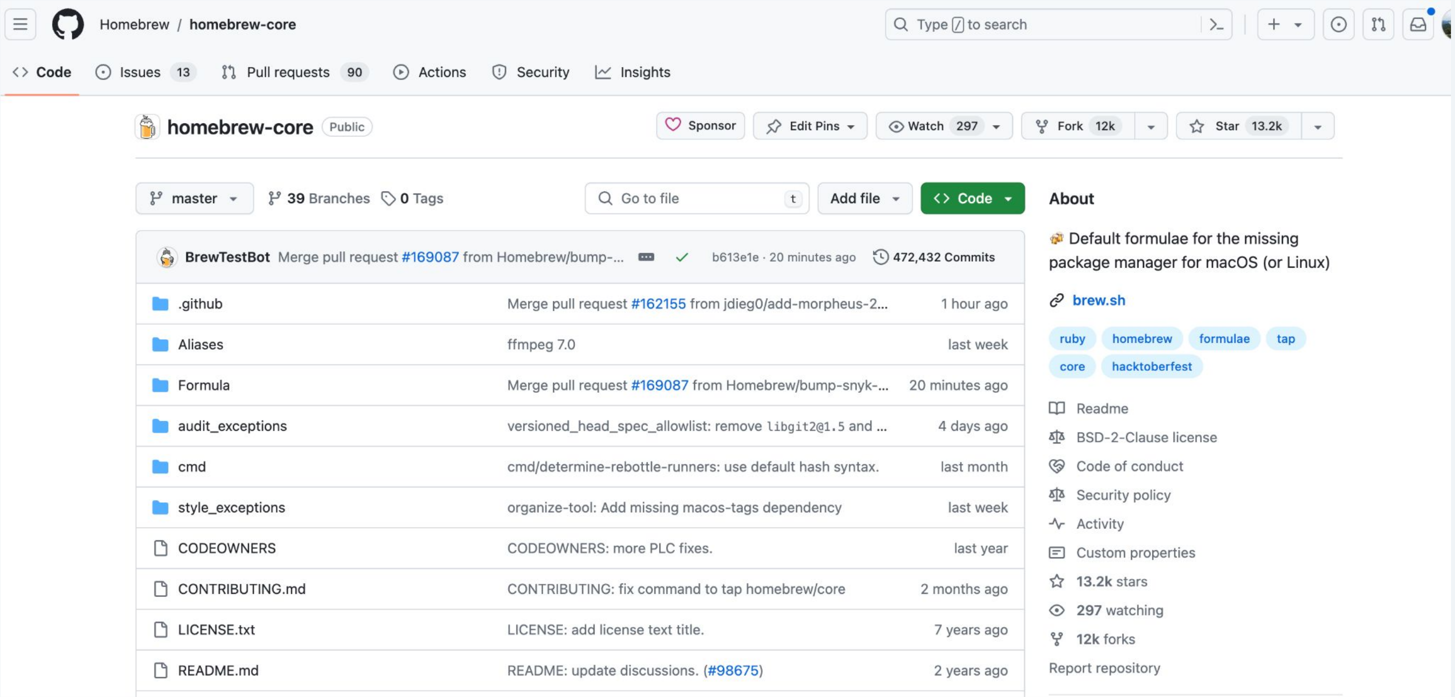
event-stream vulnerability explained

What does build provenance include?



https://slsa.dev/spec/v1.0/provenance

How are bottles built?



BrewTestBot Merge pull request #169087 from Homebrew/bump-... b613e1e · 20 minutes ago 472,432 Commits

.github	Merge pull request #162155 from jdieg0/add-morpheus-2...	1 hour ago
Aliases	ffmpeg 7.0	last week
Formula	Merge pull request #169087 from Homebrew/bump-snyk-...	20 minutes ago
audit_exceptions	versioned_head_spec_allowlist: remove `libgit2@1.5` and ...	4 days ago
cmd	cmd/determine-rebottle-runners: use default hash syntax.	last month
style_exceptions	organize-tool: Add missing macos-tags dependency	last week
CODEOWNERS	CODEOWNERS: more PLC fixes.	last year
CONTRIBUTING.md	CONTRIBUTING: fix command to tap homebrew/core	2 months ago
LICENSE.txt	LICENSE: add license text title.	7 years ago
README.md	README: update discussions. (#98675)	2 years ago

About

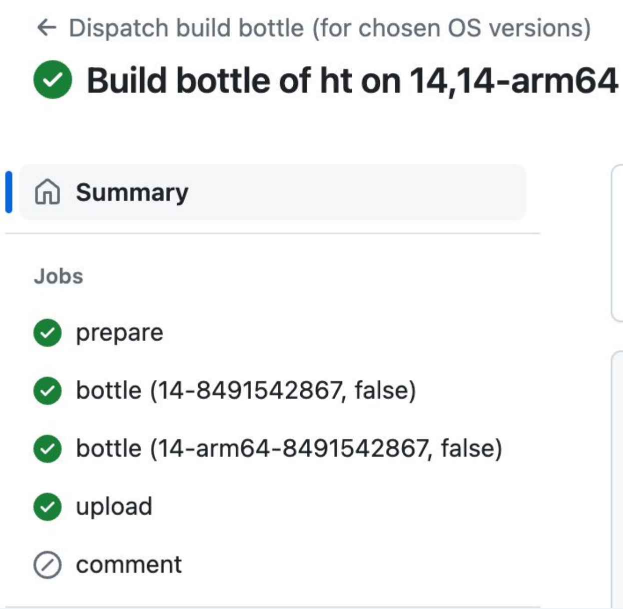
Default formulae for the missing package manager for macOS (or Linux)

brew.sh

ruby homebrew formulae tap core hacktoberfest

Readme
BSD-2-Clause license
Code of conduct
Security policy
Activity
Custom properties
13.2k stars
297 watching
12k forks
Report repository

How are bottles built?



← Dispatch build bottle (for chosen OS versions)

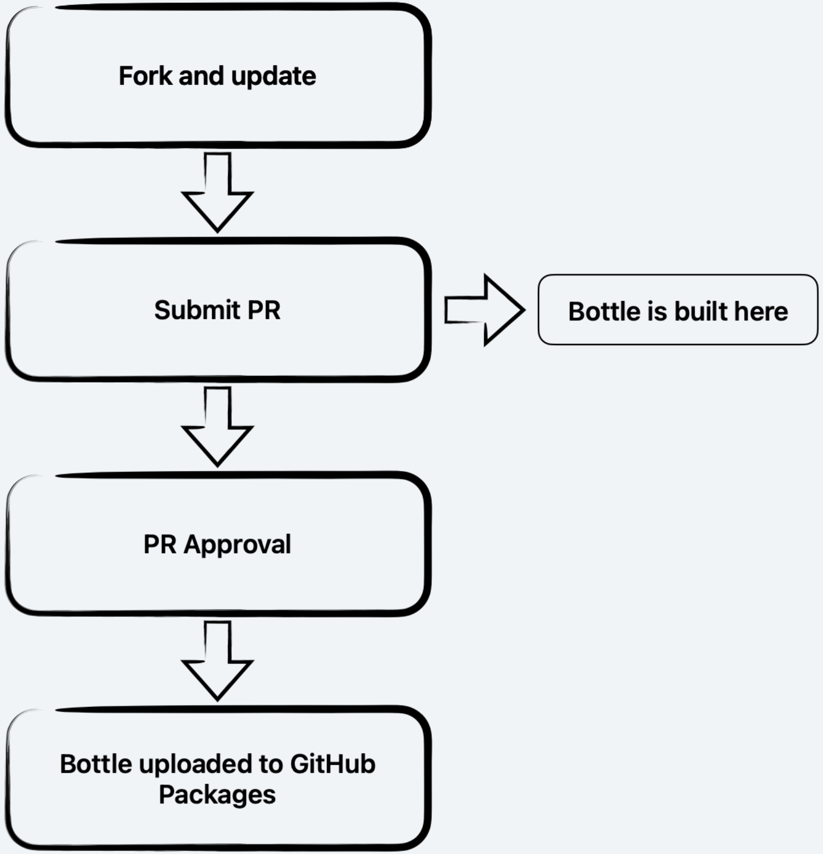
✓ **Build bottle of ht on 14,14-arm64**

Summary

Jobs

- ✓ prepare
- ✓ bottle (14-8491542867, false)
- ✓ bottle (14-arm64-8491542867, false)
- ✓ upload
- ⊘ comment

https://github.com/Homebrew/homebrew-core/actions/workflows/dispatch-build-bottle.yml



Fork and update

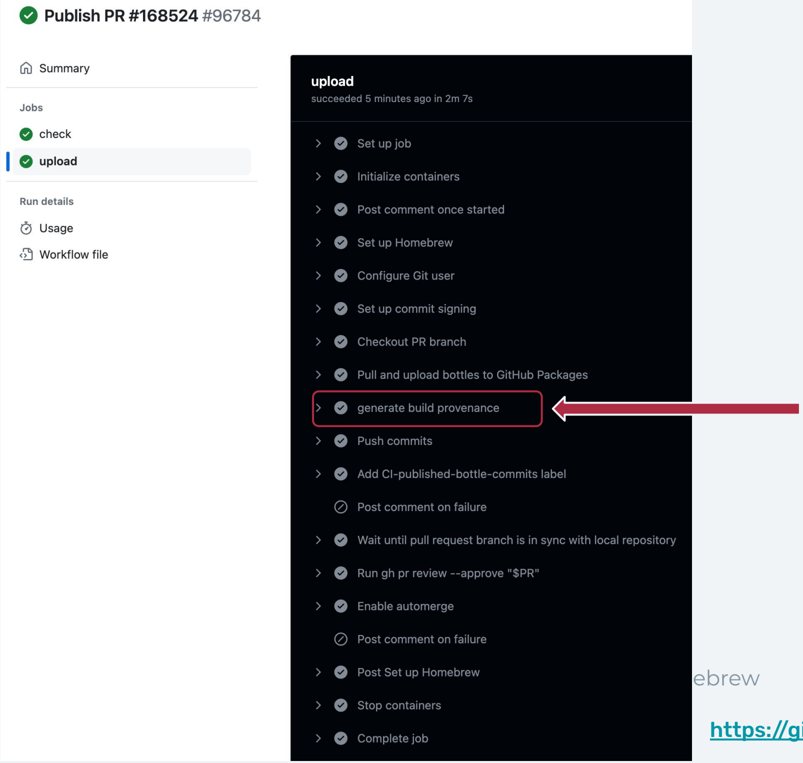
Submit PR

Bottle is built here

PR Approval

Bottle uploaded to GitHub Packages

How are bottles signed?



✓ **Publish PR #168524** #96784

- Summary

Jobs

- ✓ check
- ✓ upload

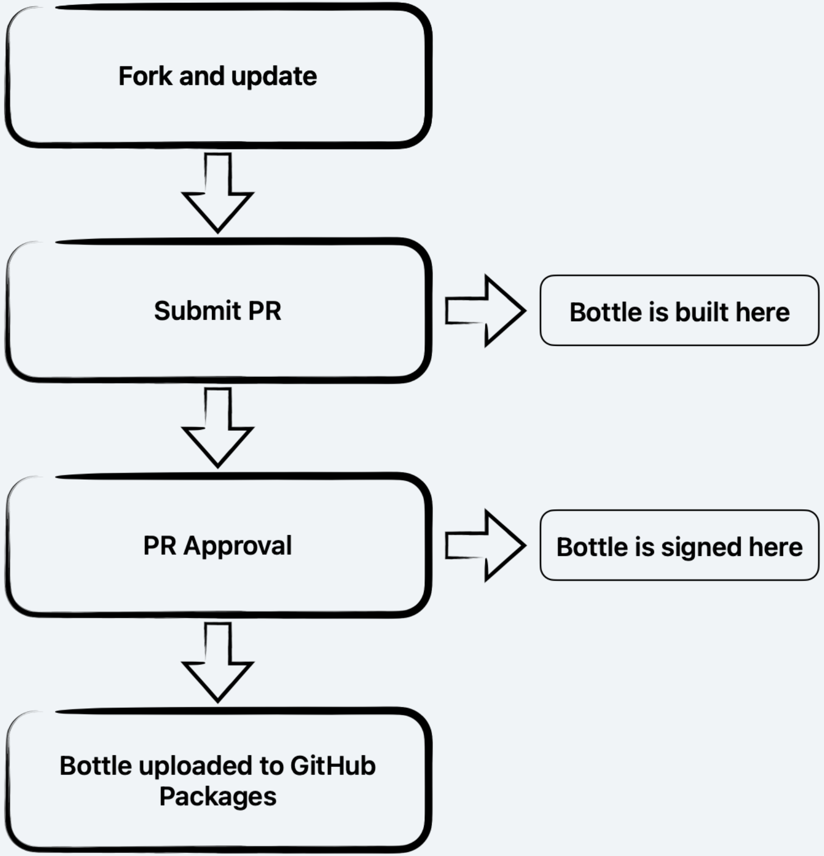
Run details

- Usage
- Workflow file

upload

succeeded 5 minutes ago in 2m 7s

- Set up job
- Initialize containers
- Post comment once started
- Set up Homebrew
- Configure Git user
- Set up commit signing
- Checkout PR branch
- Pull and upload bottles to GitHub Packages
- generate build provenance
- Push commits
- Add CI-published-bottle-commits label
- Post comment on failure
- Wait until pull request branch is in sync with local repository
- Run gh pr review --approve "$PR"
- Enable automerge
- Post comment on failure
- Post Set up Homebrew
- Stop containers
- Complete job



Fork and update

Submit PR

Bottle is built here

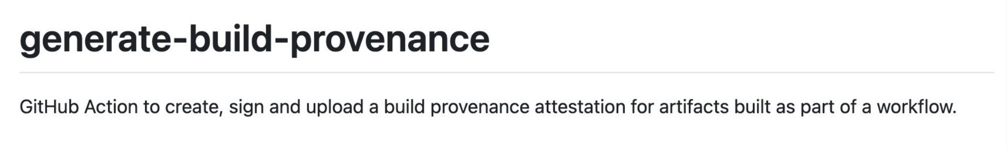
PR Approval

Bottle is signed here

Bottle uploaded to GitHub Packages

https://github.com/Homebrew/homebrew-core/actions/workflows/publish-commit-bottles.yml

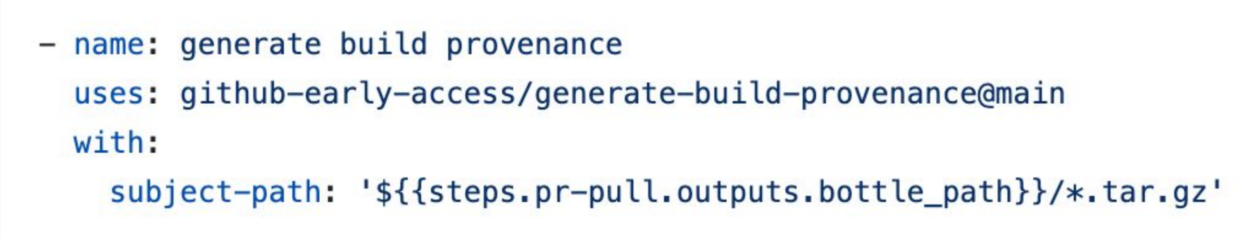
How are bottles signed?



generate-build-provenance

GitHub Action to create, sign and upload a build provenance attestation for artifacts built as part of a workflow.

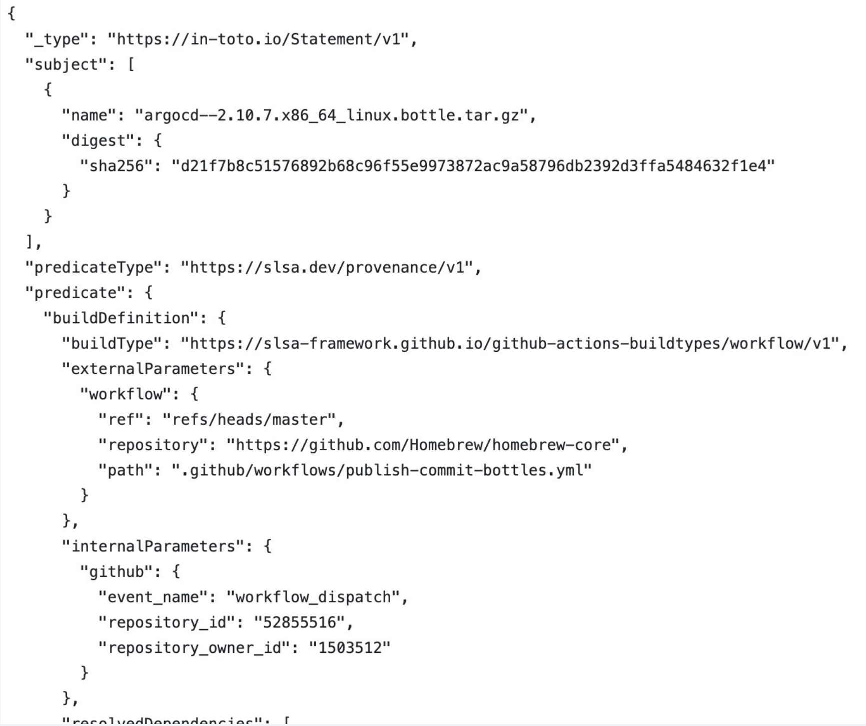
https://github.com/github-early-access/generate-build-provenance



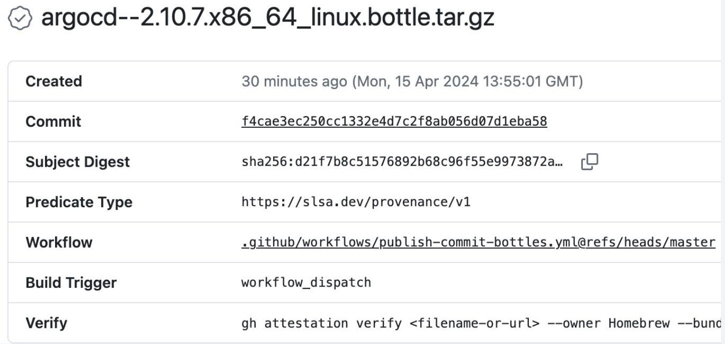
```
- name: generate build provenance
  uses: github-early-access/generate-build-provenance@main
  with:
    subject-path: '${{steps.pr-pull.outputs.bottle_path}}/*.tar.gz'
```

https://github.com/Homebrew/homebrew-core/blob/c25f04b17bcd7eadc604c4d2e737aff571e9e733/.github/workflows/publish-commit-bottles.yml#L338

So what is actually in that build provenance?

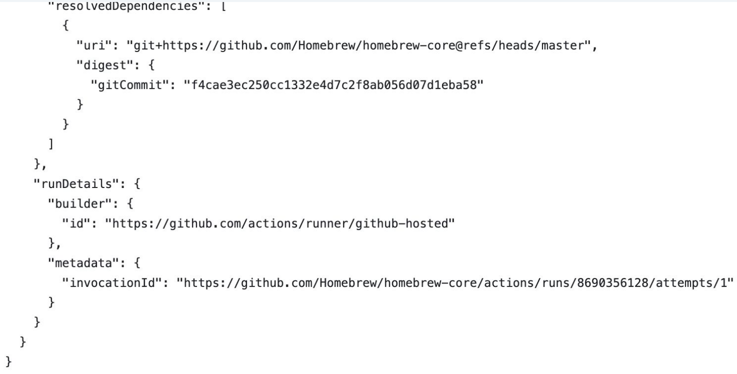


```
{
  "_type": "https://in-toto.io/Statement/v1",
  "subject": [
    {
      "name": "argocd--2.10.7.x86_64_linux.bottle.tar.gz",
      "digest": {
        "sha256": "d21f7b8c51576892b68c96f55e9973872ac9a58796db2392d3ffa5484632f1e4"
      }
    }
  ],
  "predicateType": "https://slsa.dev/provenance/v1",
  "predicate": {
    "buildDefinition": {
      "buildType": "https://slsa-framework.github.io/github-actions-buildtypes/workflow/v1",
      "externalParameters": {
        "workflow": {
          "ref": "refs/heads/master",
          "repository": "https://github.com/Homebrew/homebrew-core",
          "path": ".github/workflows/publish-commit-bottles.yml"
        }
      },
      "internalParameters": {
        "github": {
          "event_name": "workflow_dispatch",
          "repository_id": "52855516",
          "repository_owner_id": "1503512"
        }
      },
      "resolvedDependencies": [
```



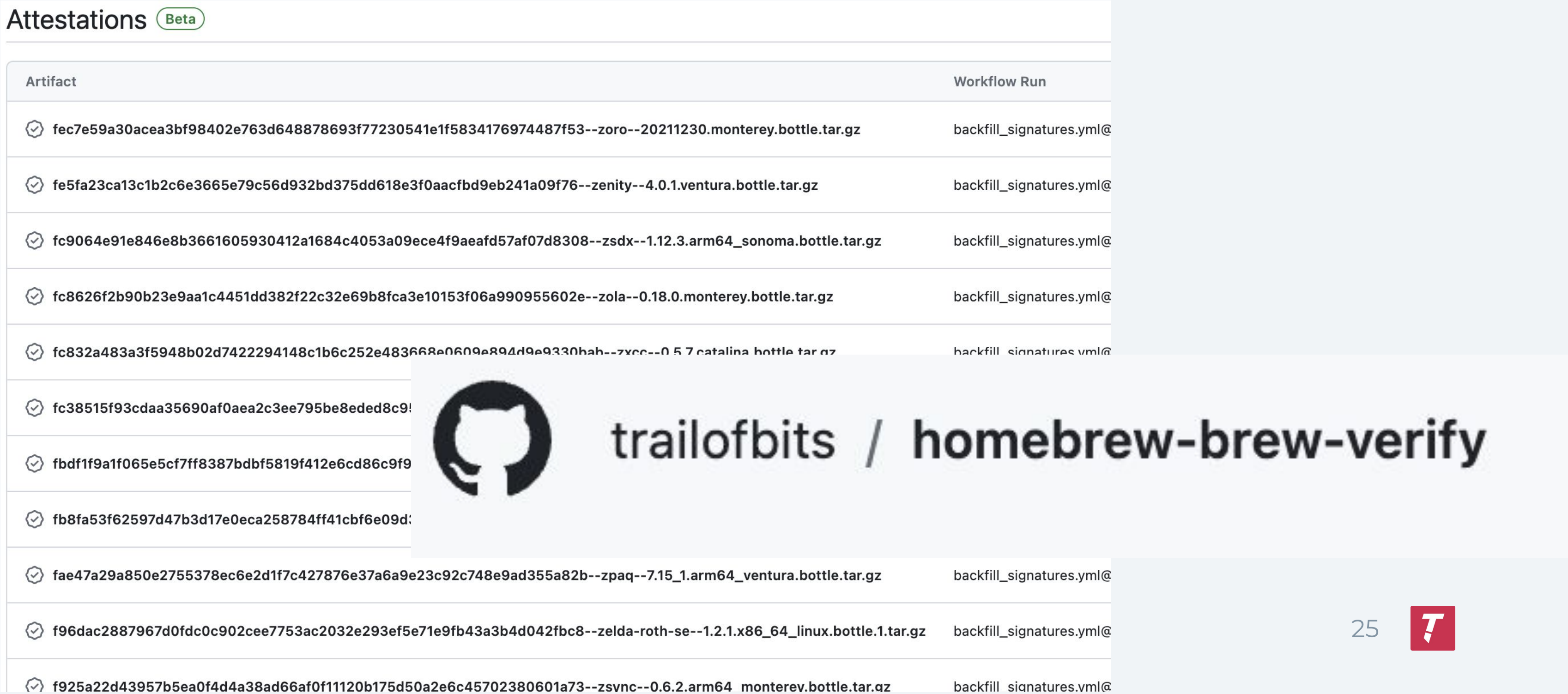
argocd--2.10.7.x86_64_linux.bottle.tar.gz

Created	30 minutes ago (Mon, 15 Apr 2024 13:55:01 GMT)
Commit	f4cae3ec250cc1332e4d7c2f8ab056d07d1eba58
Subject Digest	sha256:d21f7b8c51576892b68c96f55e9973872a…
Predicate Type	https://slsa.dev/provenance/v1
Workflow	.github/workflows/publish-commit-bottles.yml@refs/heads/master
Build Trigger	workflow_dispatch
Verify	gh attestation verify <filename-or-url> --owner Homebrew --bund



```
      "resolvedDependencies": [
        {
          "uri": "git+https://github.com/Homebrew/homebrew-core@refs/heads/master",
          "digest": {
            "gitCommit": "f4cae3ec250cc1332e4d7c2f8ab056d07d1eba58"
          }
        }
      ]
    },
    "runDetails": {
      "builder": {
        "id": "https://github.com/actions/runner/github-hosted"
      },
      "metadata": {
        "invocationId": "https://github.com/Homebrew/homebrew-core/actions/runs/8690356128/attempts/1"
      }
    }
  }
}
```

What about bottles that have already been built?

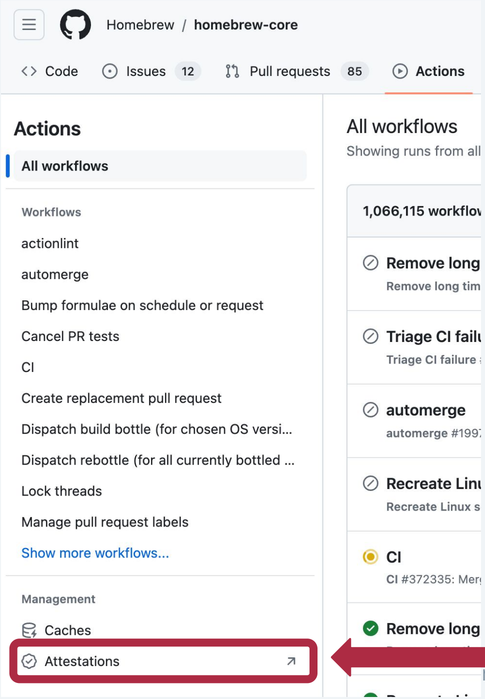


Attestations Beta

Artifact	Workflow Run
fec7e59a30acea3bf98402e763d648878693f77230541e1f5834176974487f53--zoro--20211230.monterey.bottle.tar.gz	backfill_signatures.yml@
fe5fa23ca13c1b2c6e3665e79c56d932bd375dd618e3f0aacfbd9eb241a09f76--zenity--4.0.1.ventura.bottle.tar.gz	backfill_signatures.yml@
fc9064e91e846e8b3661605930412a1684c4053a09ece4f9aeafd57af07d8308--zsdx--1.12.3.arm64_sonoma.bottle.tar.gz	backfill_signatures.yml@
fc8626f2b90b23e9aa1c4451dd382f22c32e69b8fca3e10153f06a990955602e--zola--0.18.0.monterey.bottle.tar.gz	backfill_signatures.yml@
fc832a483a3f5948b02d7422294148c1b6c252e483668e0609e894d9e9330bab--zxcc--0.5.7.catalina.bottle.tar.gz	backfill_signatures.yml@
fc38515f93cdaa35690af0aea2c3ee795be8eded8c9	
fbdf1f9a1f065e5cf7ff8387bdbf5819f412e6cd86c9f9	
fb8fa53f62597d47b3d17e0eca258784ff41cbf6e09d	
fae47a29a850e2755378ec6e2d1f7c427876e37a6a9e23c92c748e9ad355a82b--zpaq--7.15_1.arm64_ventura.bottle.tar.gz	backfill_signatures.yml@
f96dac2887967d0fdc0c902cee7753ac2032e293ef5e71e9fb43a3b4d042fbc8--zelda-roth-se--1.2.1.x86_64_linux.bottle.1.tar.gz	backfill_signatures.yml@
f925a22d43957b5ea0f4d4a38ad66af0f11120b175d50a2e6c45702380601a73--zsync--0.6.2.arm64_monterey.bottle.tar.gz	backfill_signatures.yml@

trailofbits / homebrew-brew-verify

How can I verify formula myself? The hard way.



Homebrew / homebrew-core

Code · Issues 12 · Pull requests 85 · Actions

Actions

All workflows

Workflows

- actionlint
- automerge
- Bump formulae on schedule or request
- Cancel PR tests
- CI
- Create replacement pull request
- Dispatch build bottle (for chosen OS versi...
- Dispatch rebottle (for all currently bottled ...
- Lock threads
- Manage pull request labels
- Show more workflows...

Management

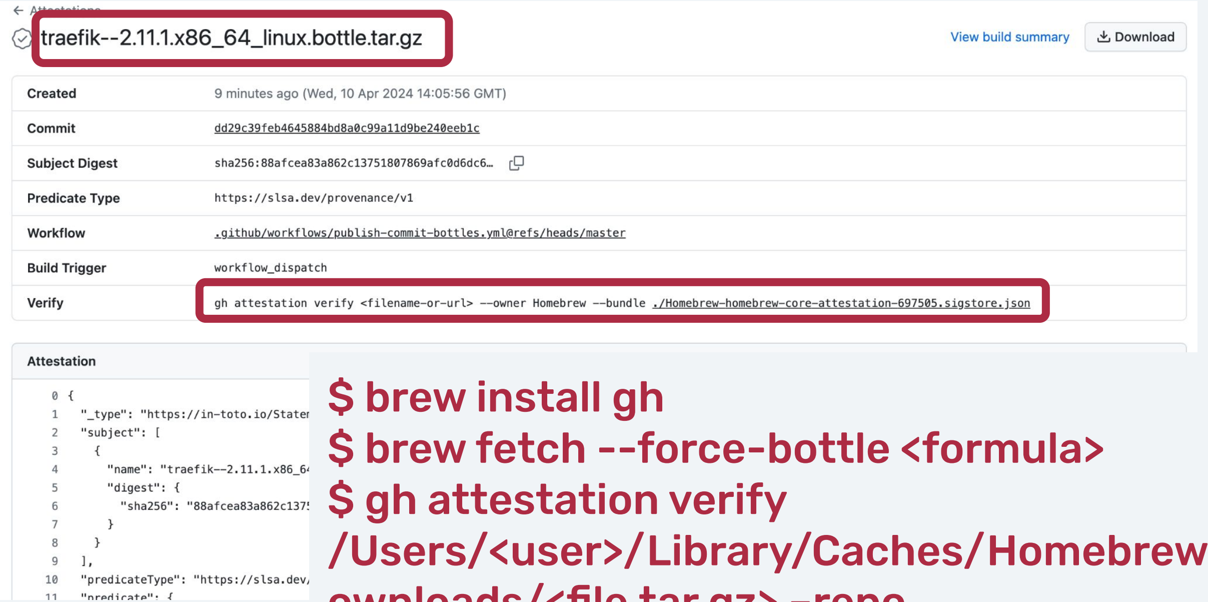
- Caches
- Attestations

All workflows

Showing runs from all

1,066,115 workflow

- Remove long
Remove long tim
- Triage CI failu
Triage CI failure
- automerge
automerge #199
- Recreate Linu
Recreate Linux s
- CI
CI #372335: Merg
- Remove long



← Attestations

traefik--2.11.1.x86_64_linux.bottle.tar.gz

View build summary · Download

Created	9 minutes ago (Wed, 10 Apr 2024 14:05:56 GMT)
Commit	dd29c39feb4645884bd8a0c99a11d9be240eeb1c
Subject Digest	sha256:88afcea83a862c13751807869afc0d6dc6…
Predicate Type	https://slsa.dev/provenance/v1
Workflow	.github/workflows/publish-commit-bottles.yml@refs/heads/master
Build Trigger	workflow_dispatch
Verify	gh attestation verify <filename-or-url> --owner Homebrew --bundle ./Homebrew-homebrew-core-attestation-697505.sigstore.json

Attestation

```
{
  "_type": "https://in-toto.io/Staten
  "subject": [
    {
      "name": "traefik--2.11.1.x86_64
      "digest": {
        "sha256": "88afcea83a862c1375
      }
    }
  ],
  "predicateType": "https://slsa.dev/
  "predicate": {
```

```
$ brew install gh
$ brew fetch --force-bottle <formula>
$ gh attestation verify /Users/<user>/Library/Caches/Homebrew/downloads/<file.tar.gz> –repo Homebrew/homebrew-core
```

How can I verify formula myself? The easy way.

```
$ brew install gh
$ brew tap trailofbits/homebrew-brew-verify
$ brew verify <formula>
```

```
$ brew verify gh
==> Downloading
https://ghcr.io/v2/homebrew/core/gh/blobs/sha256:7d3b6ad6d60935356e4657
75e9c4b1cd865275f64abfff231c6c36bb152eed88
Already downloaded:
/Users/<user>/Library/Caches/Homebrew/downloads/384a5ba1dd3c1b02d4bed
ea48f1676981161a8a8c27550e2a4a4ee2ceb5fc716--gh--2.47.0.arm64_sonoma.b
ottle.tar.gz
==> Verified gh with tag arm64_sonoma.
```

How can I verify formula myself? The (future) easy way.

```
$ brew verify <formula>
```

or

```
$ brew install <formula>
```

now

```
$ HOMEBREW_VERIFY_ATTESTATIONS=1 brew install
```

https://github.com/Homebrew/brew/pull/17049

Acknowledgements

- **Alpha-Omega of the OpenSSF**
  - Michael Winser
- **The Homebrew Maintainers:**
  - @MikeMcQuaid
  - @carlocab
  - @Bo98
  - Everyone else that helped and provided valuable feedback along the way.
- **The GitHub Package Security Team**
  - Phillip Mendonça-Vieira
  - Trevor Rosen
  - Everyone else that helped ship these features.
- **Will Woodruff - Trail of Bits**

Thank You!

- **Reach out**
  - joe.sweeney@trailofbits.com
- **Links**
  - Trail of Bits Blog
  - Alpha-Omega Blog
- **Technical Links**
  - brew verify repository
  - Follow the work on GitHub
    - Issue for attestation verification in `brew install`
  - Build Provenance Architecture Doc