Breaking Build

Red Teaming CI/CD Pipelines and GitHub Actions

BSIDES PORTLAND 2024

HELLO!

- **Craig Wright**
- @werdhaihai
- Adversary Simulation Consultant
- Pretend to be a professional chef

Agenda

- Introduction to CI/CD
- Attacking CI/CD
- Deep Dive into GitHub Actions
- Demo
- Defensive Strategies

Introduction to CI/CD

What is a CI/CD Pipeline??

… set of systems which enable repeatable and automated way to analyze, test, integrate, build, and deliver code

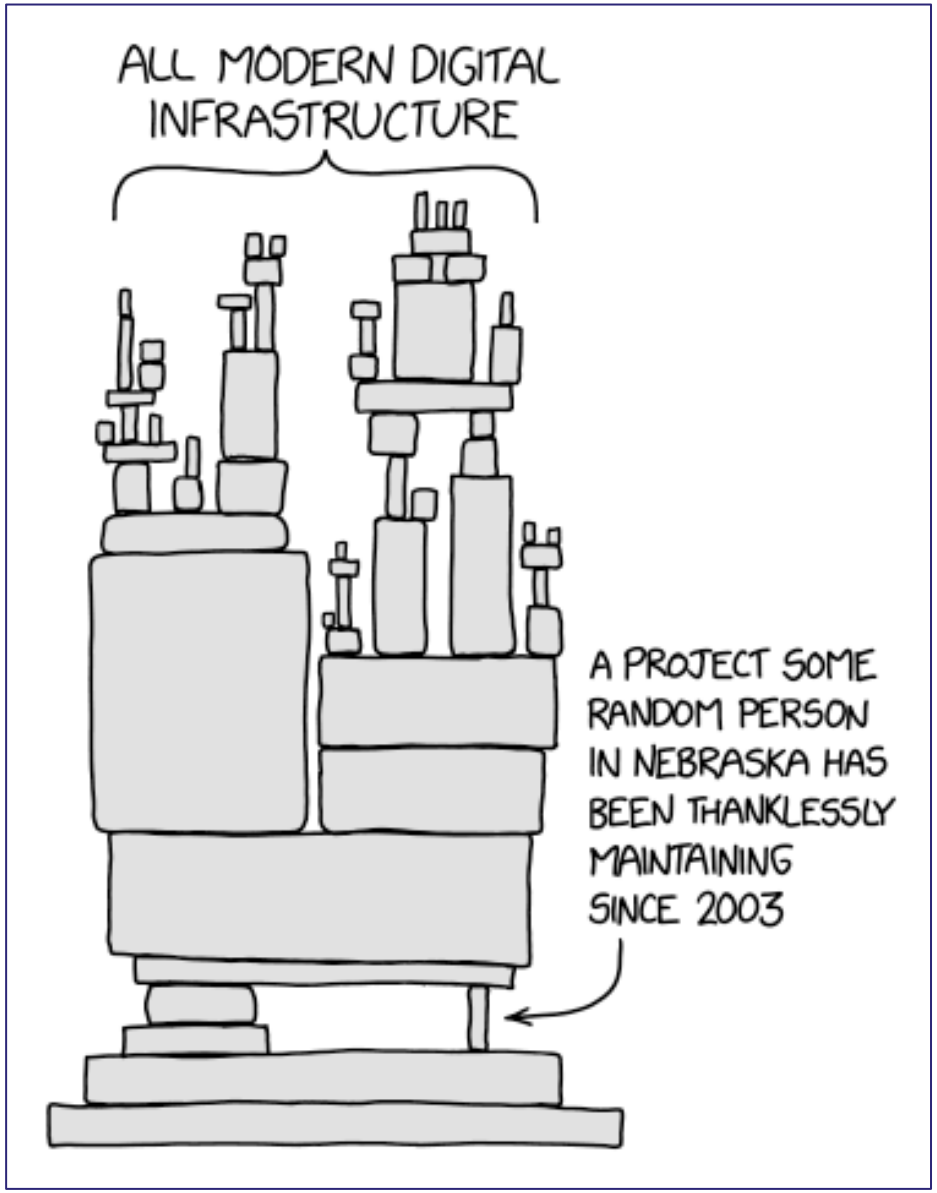
Ok… so wtf is it?

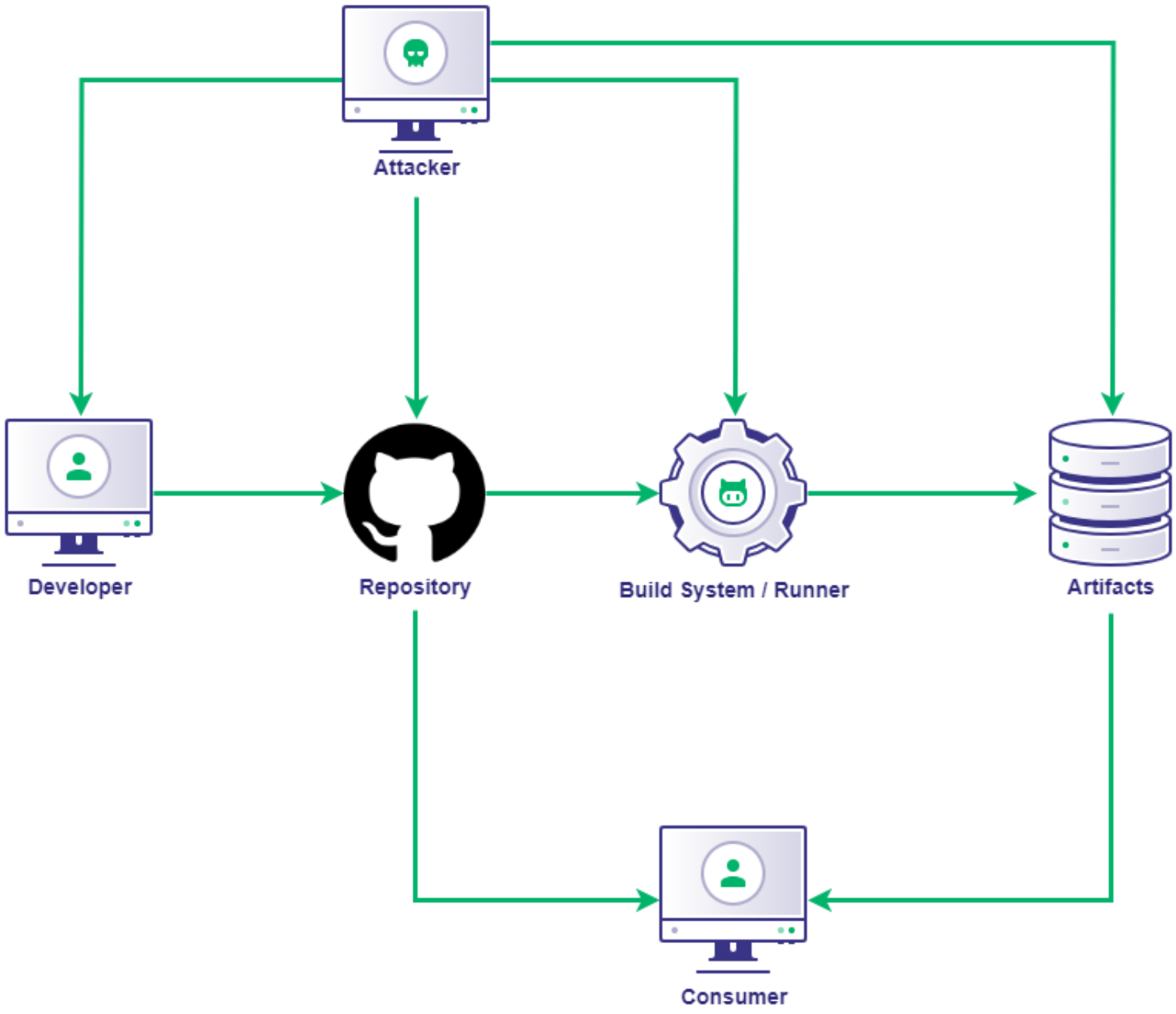
- Version Control System
- Continuous Integration Systems
- Deployment Pipeline/Systems
- Artifact Repository

Attacking CI/CD

What's the Attack Surface

- Developers
- Repositories
- Third party dependencies 😱
- Build systems
- Artifact Storage



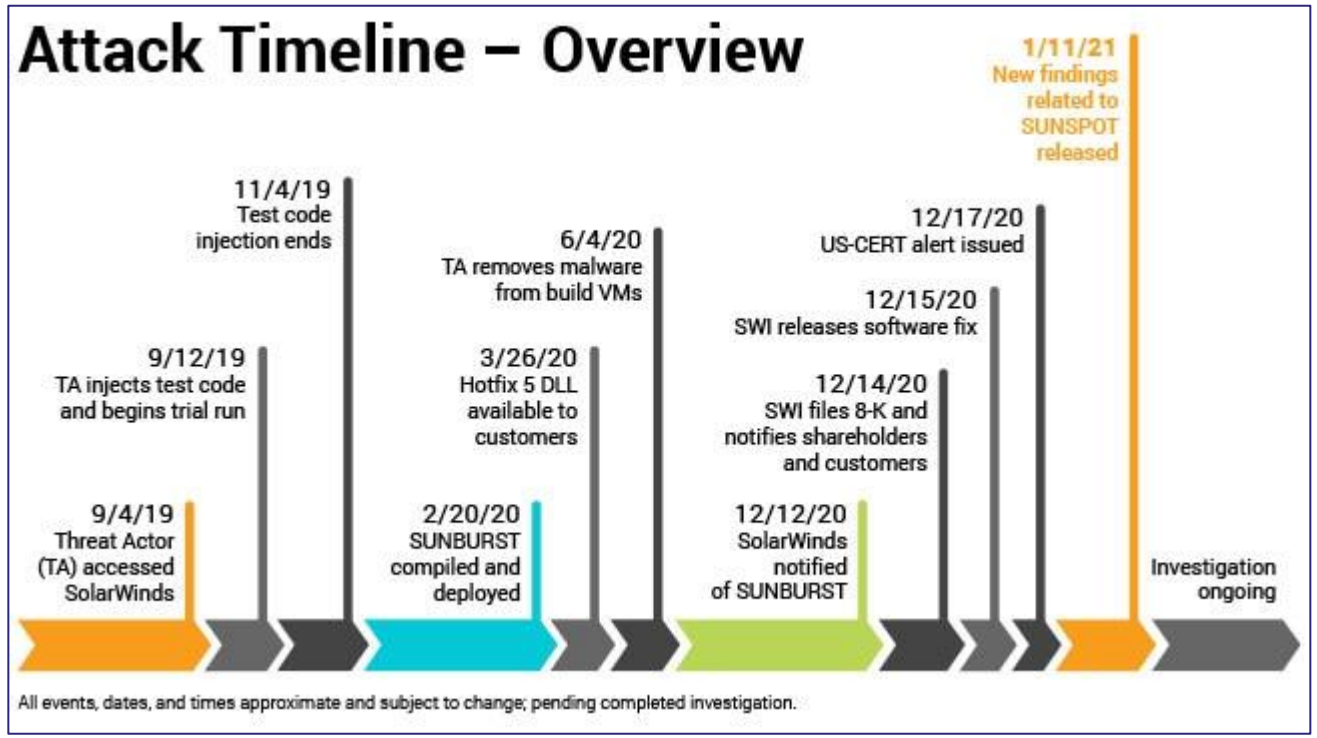

Attacker
Developer
Repository
Build System / Runner
Artifacts
Consumer

Sh*t Gets Real (World)

- Solar Winds
- xz

SolarWinds 🙄 😴

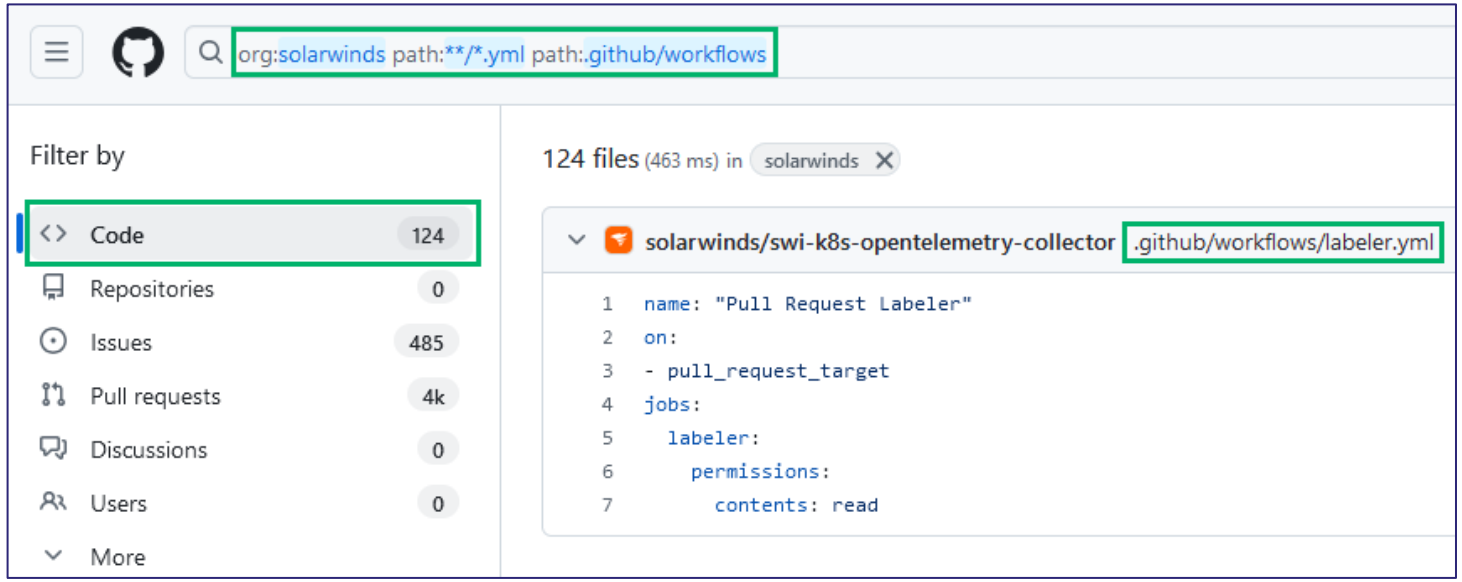
- Consists of two components
  - *SUNSPOT* (inserts the *SUNBURST* backdoor)
  - *SUNBURST* (Backdoor to establish C2 to APT29)
- *SUNSPOT* ran as a Scheduled Task on build systems
- Monitored for MSBUILD.EXE replaced code at compilation time
- Injected backdoored code compiled into a DLL
- SUNBURST traffic mimics legitimate ORION traffic

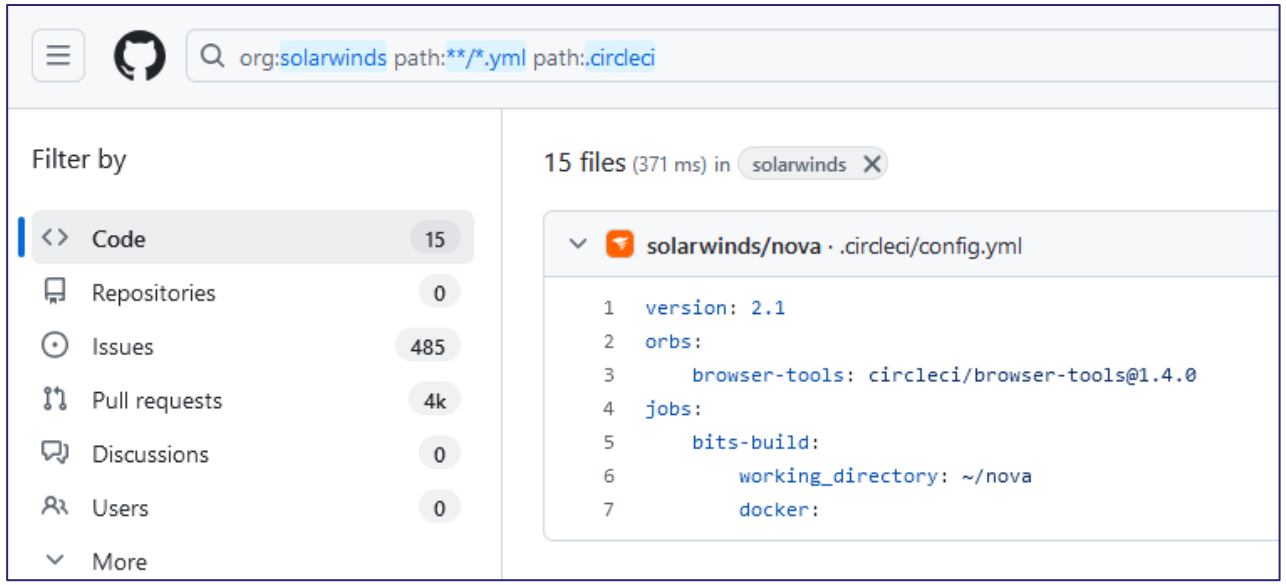


https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/
https://cloud.google.com/blog/topics/threat-intelligence/sunburst-additional-technical-details/

SolarWinds

- GitHub search reveals the use of GitHub Actions and CircleCI

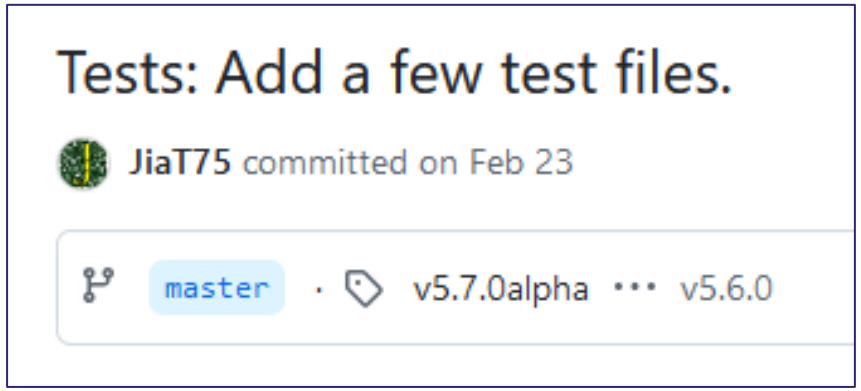


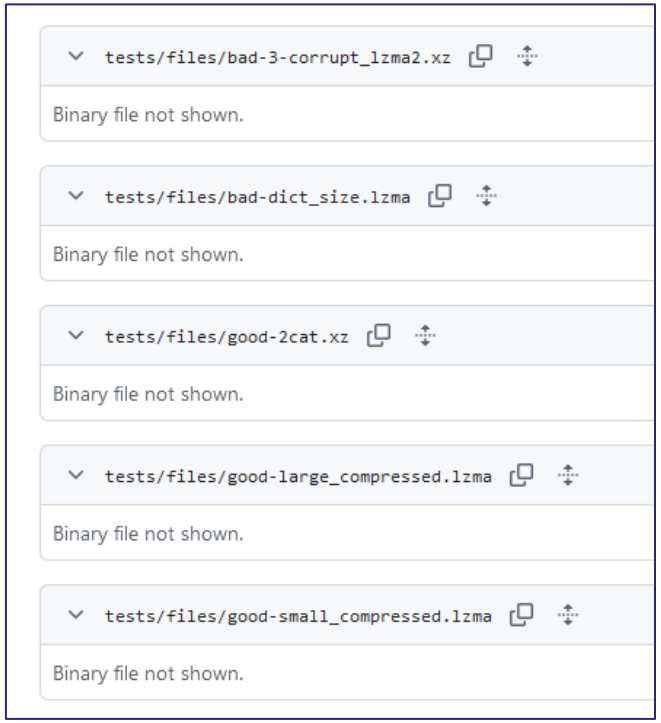


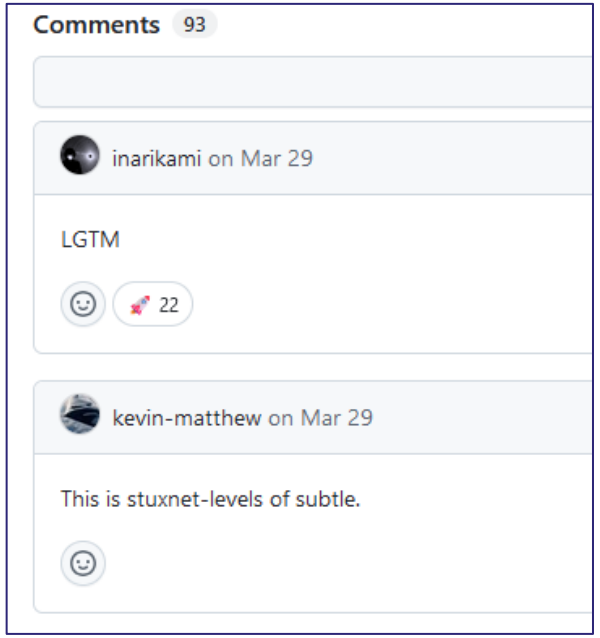
xz (CVE-2024-3094)

a helpful dev PRs a NULL check

- Consisted of a shell script and an object file
- The shell script modified the build process to backdoor artifacts
- Backdoored artifacts built for Linux distributions







xz (CVE-2024-3094)

xz / .github / workflows /

thesamesam and Larhzu CI: update FreeBSD, NetBSD, OpenBSD, Solaris actions

Name
..
ci.yml
freebsd.yml
netbsd.yml
openbsd.yml
solaris.yml
windows-ci.yml

Commits on Dec 30, 2022

CI/CD: Create initial version of CI/CD workflow.

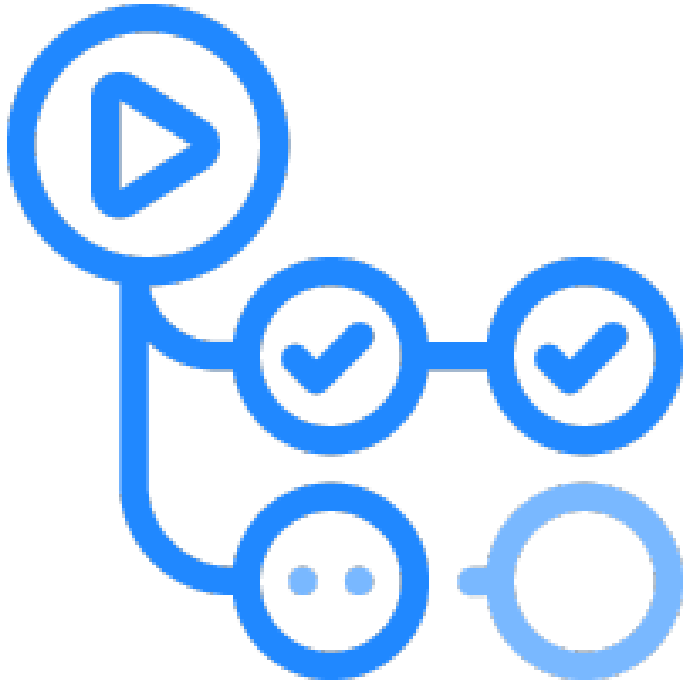
JiaT75 committed on Dec 30, 2022

End of commit history for this file

GitHub Actions

GitHub Actions Terminology

- **GitHub Actions** – GitHub's CI/CD "platform"
- **Workflows** – YAML files used to define jobs
- **Events** – Activity that triggers a workflow
- **Jobs** – Set of steps to be executed on the runner
- **Actions** – Reusable tasks used in workflows
- **Runner** – a server that runs a build



Workflows

- YAML configuration used to define a Job
- Found in *.github/workflows/* directory
- Triggered by an event or on a schedule
- Repositories can contain many of these

```yaml
name: PR Slack Notification

on:
  pull_request:
    types: [opened, synchronize]

jobs:
  notify:
    runs-on: ubuntu-latest
    steps:
      - name: Send Slack notification
        uses: slackapi/slack-github-action@v1.27.0
        with:
          slack-message: "A pull request has been opened: ${{ github.event.pull_request.html_url }}"
          slack-webhook: ${{ secrets.SLACK_WEBHOOK }}
```

Events

- The trigger for a workflow
- Many events can be used to trigger a workflow
  - Issues
  - Pull Request
  - Releases
  - Schedule

```yaml
name: PR Slack Notification

on:
  pull_request:
    types: [opened, synchronize]

jobs:
  notify:
    runs-on: ubuntu-latest
    steps:
      - name: Send Slack notification
        uses: slackapi/slack-github-action@v1.27.0
        with:
          slack-message: "A pull request has been opened: ${{ github.event.pull_request.html_url }}"
          slack-webhook: ${{ secrets.SLACK_WEBHOOK }}
```

Jobs and Steps

- Jobs are a collection of steps
- Steps either a shell script or an action

```yaml
name: PR Slack Notification

on:
  pull_request:
    types: [opened, synchronize]

jobs:
  notify:
    runs-on: ubuntu-latest
    steps:
      - name: Send Slack notification
        uses: slackapi/slack-github-action@v1.27.0
        with:
          slack-message: "A pull request has been opened: ${{ github.event.pull_request.html_url }}"
          slack-webhook: ${{ secrets.SLACK_WEBHOOK }}
```

Actions

- Actions are applications used in workflows
- Provide a way to simplify otherwise complex tasks

```yaml
name: PR Slack Notification

on:
  pull_request:
    types: [opened, synchronize]

jobs:
  notify:
    runs-on: ubuntu-latest
    steps:
      - name: Send Slack notification
        uses: slackapi/slack-github-action@v1.27.0
        with:
          slack-message: "A pull request has been opened: ${{ github.event.pull_request.html_url }}"
          slack-webhook: ${{ secrets.SLACK_WEBHOOK }}
```

Actions

slackapi / slack-github-action

Code | Issues 31 | Pull requests 2 | Actions | Security | Insights

slack-github-action Public

Watch 25 | Fork 147 | Star 944

Use this GitHub action with your project
Add this Action to an existing workflow or create a new one

View on Marketplace

main | Go to file | Code

zimeg docs(fix): reference octokit context and ... 43604b7 · last week

.github	ci: include the slack health sco...	3 weeks ago
example-workflows	chore(release): tag version 1.2...	2 months ago
src	feat: make the payload delimit...	2 months ago
test	feat: make the payload delimit...	2 months ago

About

Send data into Slack using this GitHub Action!

slack | bot | github-actions

Readme
MIT license
Activity
Custom properties
944 stars
25 watching
147 forks

Actions

main | slack-github-action / action.yml

rzumer and zimeg feat: make the payload delimiter configurable for workflow webhook tr...

Code | Blame | 37 lines (37 loc) · 2.26 KB

```yaml
name: 'slack-send'
description: 'Publish a message in a channel or send a JSON payload to the Slack Workflow Builder'
inputs:
  channel-id: # channel id to post message when using bot token
    description: 'Slack channel ID where message will be posted. Needed if using bot token'
    required: false
  slack-message: # message to post when using bot token
    description: 'Message to post into Slack. Needed if using bot token'
    required: false
  payload: # JSON payload to send to Slack via webhook
    description: 'JSON payload to send to Slack if webhook route. If not supplied, json from GitHub
    required: false
  payload-delimiter: # custom delimiter used to flatten nested values in the JSON payload
    description: 'Custom delimiter used to flatten nested values in the JSON payload. If not suppli
```

Runners

GitHub Hosted Runners

- Free (for a bit)
- Short-lived Ephemeral
- Managed and Maintained by GitHub

Self-Hosted Runners

- Free to use
- Persistent hosts
- Managed and Maintained by you

"We recommend that you only use self-hosted runners with private repositories."

Attacks

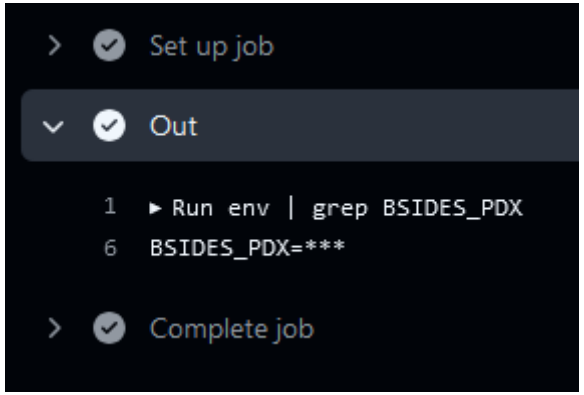
Stealing Secrets

- Secrets can be scoped to Repository or Organization
- Secrets are available regardless of branch protection
- GitHub attempts to prevent exposure of these in runner logs, but they're pretty easy to get

```yaml
name: secrets

on: [push]

jobs:
  secret_job:
    runs-on: ubuntu-latest
    env:
      BSIDES_PDX: ${{ secrets.BSIDES_PDX }}
    steps:
    - name: Out
      run: env | grep BSIDES_PDX
```



Event Context Injection

- Values controlled by a user passed directly into command interpreter
- Several events can contain attacker-controlled data

```yaml
name: Check Issue Title

on:
  issues:
    types: [opened, edited]

permissions:
  issues: write

jobs:
  validate_issue_title:
    runs-on: ubuntu-latest
    env:
      GH_TOKEN: ${{ secrets.GITHUB_TOKEN }}
    steps:
      - name: Check Issue Title Format
        run: |
          title=${{ github.event.issue.title }}
          echo "Validating issue title format..."

          # Check if issue title is appropriately titled
          if [[ $title == Bug:* ]]; then
            echo "Title format is valid."
          else
            echo "Title did not meet the required format."

            comment="Title validation failed: $title does not follow the expected format."

            # Post a comment with the output, which contains the issue title
            gh api repos/${{ github.repository }}/issues/${{ github.event.issue.number }}/comments \
              -f body="Validation failed: $comment"
          fi
```

Inject you own Workflows!

*… forks of your public repository **can** potentially run **dangerous code on your self-hosted runner** machine by creating a pull request that executes the code in a workflow*

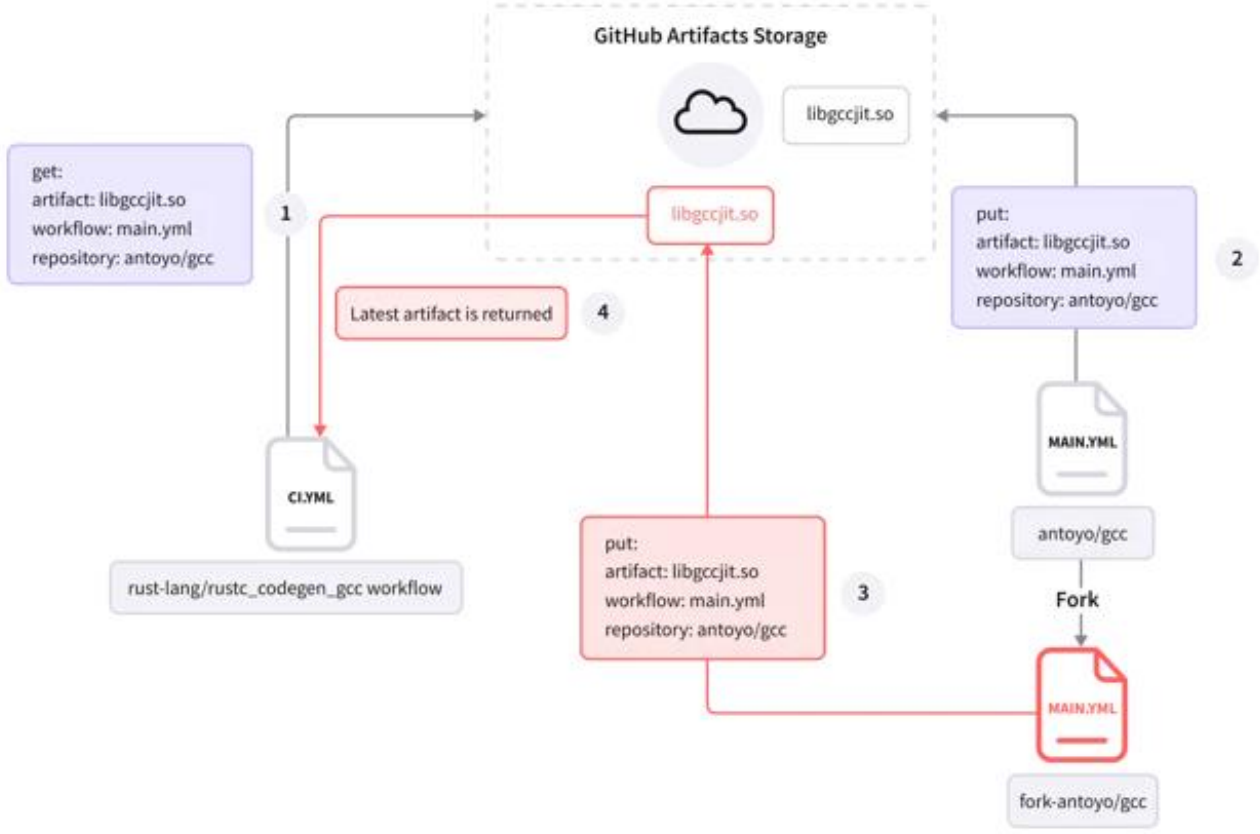
- It's simple, just get a pull request merged into main to become a Contributor
- Create a workflow for pull requests
- Make a pull request
- Have code execute on THEIR runner

Artifact Poisoning

- Artifacts can be poisoned during the build process by modifying:
  - third-party components
  - source code
  - compiled code
- These artifacts can be consumed downstream
- Implementation varies wildly based on language, platform, etc.

Artifact Poisoning

The problem
"The "download artifacts" API … doesn't differentiate between artifacts that were uploaded by forked repositories and base repositories"



GitHub Artifact Poisoning Map

Cache Poisoning

- The *actions/cache* action provides a way to speed up workflows by storing a copy of dependencies
- If attackers compromise a runner, the cache can be modified to use a backdoored dependency
- Challenging to pull off and prone to error
- You'll probably break everything

The Monsters in Your Build Cache – GitHub Actions Cache Poisoning

Published by adnanthekhan on May 6, 2024

Don't Accidentally Break Everything!

Success…but I broke everything.

Demo

Stealing Secrets

werdhaihai / typoTime

Type / to search

Code | Issues 1 | Pull requests | Actions | Projects | Security | Insights | Settings

typoTime

Private

Unwatch 1 | Fork 0 | Star 0

main | 5 Branches | Tags | Go to file t | Add file | Code

werdhaihai Update secrets.yml ✕ 813552c · 20 hours ago 34 Commits

.github/workflows	Update secrets.yml	20 hours ago
README.md	Initial commit	last week

README

typoTime

Typo Time

About

Typo Time

Readme
Activity
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Event Injection

typoTime

Private

Unwatch 1 Fork 0 Star 0

main 5 Branches Tags Go to file t Add file Code

werdhaihai Update check-issue-title.yml b5a724c · 3 minutes ago 39 Commits

.github/workflows	Update check-issue-title.yml	3 minutes ago
README.md	Initial commit	last week

README

typoTime

Typo Time

About

Typo Time

Readme
Activity
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Pull Request Workflow Injection

Applications snoitca/githubActionsBSi... New Tab - Google Chrome pull-request.yml - Actions ... 2024-10-23 06:16 PM defaultuser

snoitca/githubActionsBSid

https://github.com/snoitca/githubActionsBSidesPDX 120%

snoitca / **githubActionsBSidesPDX**

Type / to search

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

githubActionsBSidesPDX Public

Pin Unwatch 1 Fork 0 Star 0

main 1 Branch Tags Go to file t Add file Code

snoitca Create verify-runner.yml ✓ 210ccec · 1 hour ago 3 Commits

.github/workflows	Create verify-runner.yml	1 hour ago
README.md	Update README.md	2 hours ago

README

githubActionsBSidesPDX

A super awesome repositoryy.

About

No description, website, or topics provided.

Readme
Activity
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

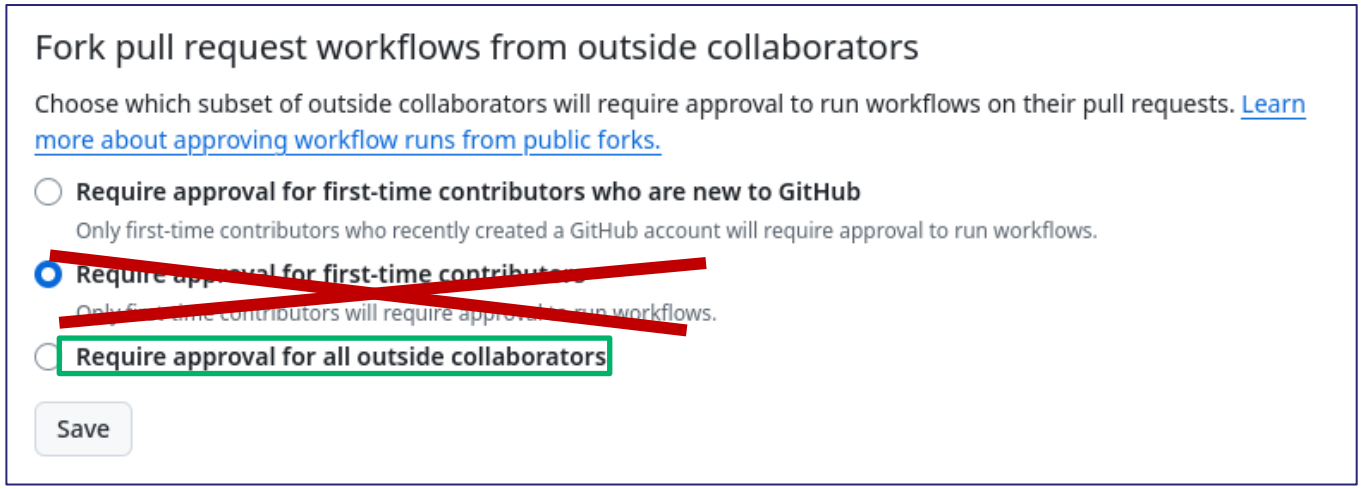
No packages published
Publish your first package

Defensive Strategies

GitHub Actions Security

Runners

- NEVER run a self-hosted runner on a Public repository!
- Restrict network access as much as possible



Self-hosted runner security

We recommend that you only use self-hosted runners with private repositories. This is because forks of your public repository can potentially run dangerous code on your self-hosted runner machine by creating a pull request that executes the code in a workflow.

GitHub Actions Security

Repositories

- Use a CODEOWNERS file to protect *.github/* directory and other sensitive files
- Enforce commit signing (preferably with hardware tokens)
- Enable branch protection

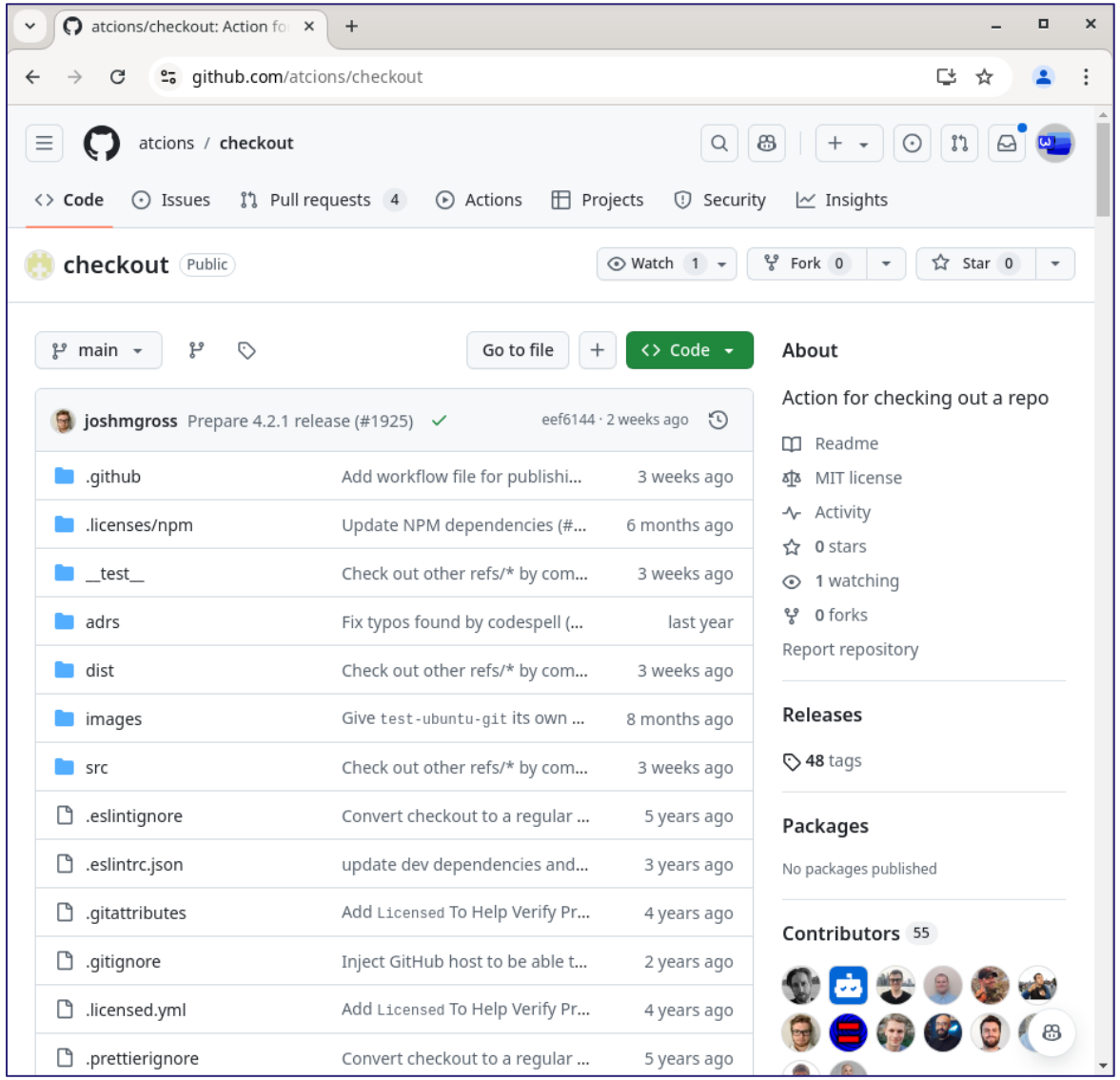
About code owners

You can use a CODEOWNERS file to define individuals or teams that are responsible for code in a repository.

GitHub Actions Security

Actions

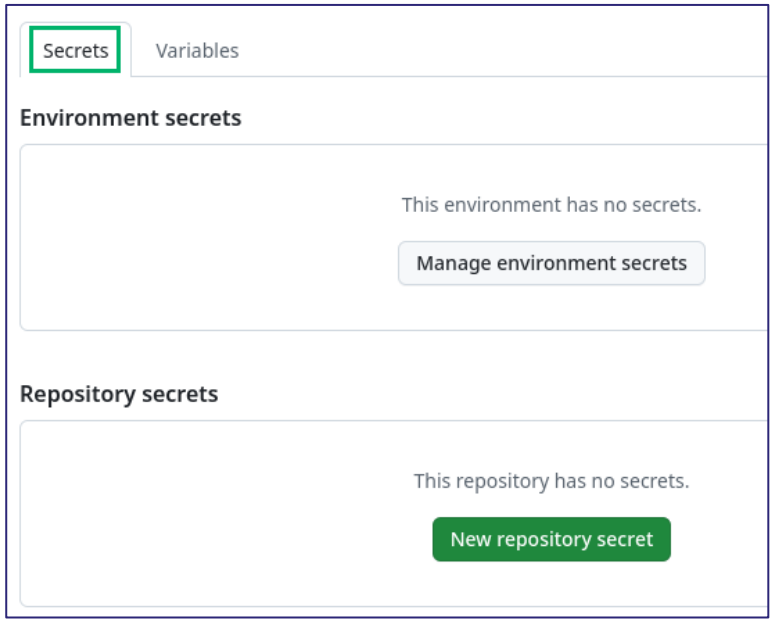
- Use caution with untrusted actions
- Always use the latest version of trusted actions



GitHub Actions Security

Secrets and GitHub Tokens

- Use secrets, not variables
- Limit scope of secrets and tokens in line with principle of least privilege




```
JWT_SECRET_KEY=${{ vars.JWT_SECRET_KEY }}
JWT_REFRESH_KEY=${{ vars.JWT_REFRESH_KEY }}
JWT_VERIFY_USER_LINK_TOKEN_EXPIRED=${{ vars.JWT_VERIFY_USER_LINK_TOKEN_EXPIRED }}
JWT_TOKEN_EXPIRED=${{ vars.JWT_TOKEN_EXPIRED }}
JWT_REFRESH_EXPIRED=${{ vars.JWT_REFRESH_EXPIRED }}
REDIS_HOST=
RESEND_TOKEN=${{ vars.RESEND_TOKEN }}
RESEND_EMAIL_DOMAIN=${{ vars.RESEND_EMAIL_DOMAIN }}
AWS_ACCESS_KEY=${{ vars.AWS_ACCESS_KEY }}
AWS_SECRET_ACCESS_KEY=${{ vars.AWS_SECRET_ACCESS_KEY }}
AWS_REGION=${{ vars.AWS_REGION }}
AWS_S3_BUCKET=${{ vars.AWS_S3_BUCKET }}
REPLICATE_API_TOKEN=${{ vars.REPLICATE_API_TOKEN }}
OPEN_API_KEY=${{ vars.OPEN_API_KEY }}
```

Acknowledgements

Shoutout

- Adnan Khan / AdnaneKhan
- John Stawinski / jstawinski

python 3.10+ code style black

Gato (Github Attack TOolkit) - Extreme Edition

Gato-X is a *FAST* scanning and attack tool for GitHub Actions pipelines. You can use it to identify Pwn Requests, Actions Injection, TOCTOU Vulnerabilities, and Self-Hosted Runner takeover at scale using just a single API token.

SPECTEROPS

Thank you