

Hack din egen pipeline

Cloud Native Day Bergen 2025



[in](https://www.linkedin.com/in/emilalbrektsson)/emilalbrektsson



[in](https://www.linkedin.com/in/jksolbakken)/jksolbakken

A professional portrait of a bald man with blue eyes, wearing a dark grey suit jacket over a white shirt and a dark tie. He is looking directly at the viewer with a serious, intense expression. The background is solid black.

Har DU trusselmodellert dine pipelines?

The malicious package versions contain a worm that executes a post-installation script. This malware scans the compromised environment for sensitive credentials, including:

- .npmrc files (for npm tokens)
- Environment variables and configuration files specifically targeting GitHub Personal Access Tokens (PATs) and API keys for cloud services like:
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
 - Microsoft Azure

Token Exfiltration Campaign via GitHub Actions Workflows

Summary

I recently responded to an attack campaign where malicious actors injected code into GitHub Actions workflows attempting to steal PyPI publishing tokens. PyPI was not compromised, and no PyPI packages were published by the attackers.

News

News

ctrl/tinycolor and 40+ NPM Packages Compromised

The popular @ctrl/tinycolor package with over 2 million weekly downloads has been compromised alongside 40+ other NPM packages in a sophisticated supply chain attack dubbed "Shai-Hulud". The malware self-propagates across maintainer packages, harvests AWS/GCP/Azure credentials using TruffleHog, and establishes persistence through GitHub Actions backdoors - representing a major escalation in NPM ecosystem threats.

Harden-Runner detection: tj-actions/changed-files action is compromised



Software packages with more than 2 billion weekly downloads hit in supply-chain attack

Incident hitting npm users is likely the biggest supply-chain attack ever.

Compromised SpotBugs Token Led to GitHub Actions Supply Chain Hack

Evidence shows a SpotBugs token compromised in December 2024 was used in the March 2025 GitHub Actions supply chain attack.

GitHub Action Compromise Puts CI/CD Secrets at Risk in Over 23,000 Repositories

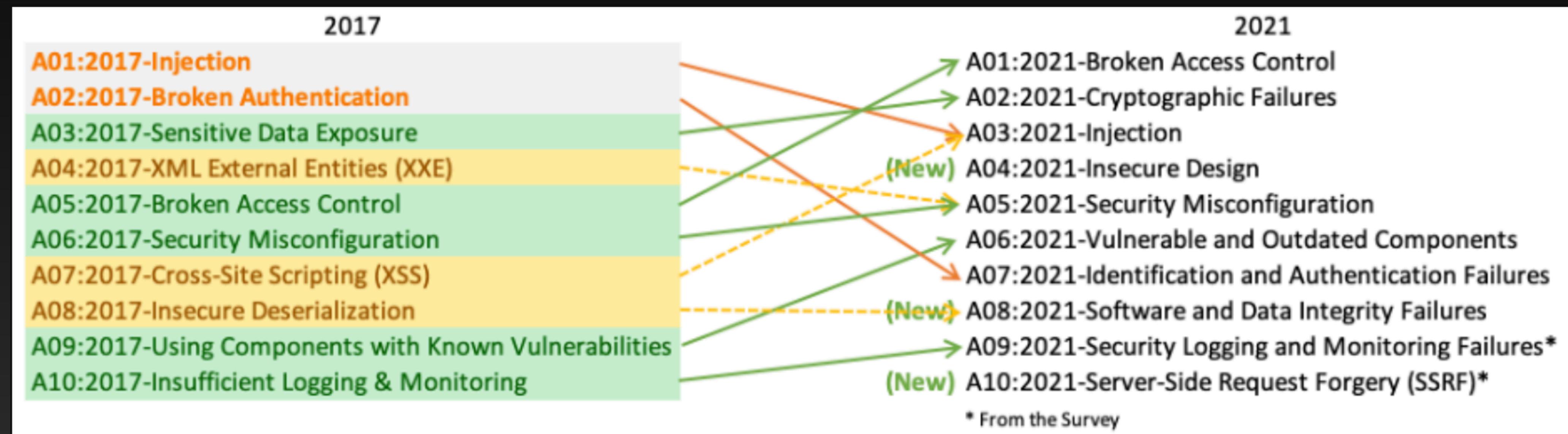
Nx S1ngularity

Shell injection in GitHub Action with `pull_request_target` trigger and unnecessary read/write permissions¹, used to extract a npm token.

Root cause: `pull_request_target`.

Contributing factors: read/write CI permissions, long-lived credential exfiltration, post-install scripts.

Trusler



Kompromitterte credentials

```
- name: Log in to registry
  run: echo "${{ secrets.GITHUB_TOKEN }}" | docker login ghcr.io -u ${{ github.actor }} --password-stdin
```

GITHUB_TOKEN

Learn what `GITHUB_TOKEN` is, how it works, and why it matters for secure automation in GitHub Actions workflows.

The screenshot shows the GitHub Developer Settings interface. On the left, a sidebar lists 'GitHub Apps', 'OAuth Apps', 'Personal access tokens' (selected), 'Fine-grained tokens', and 'Tokens (classic)'. The main area displays a token named 'demo-token' with the following details:

- Scopes: `admin:enterprise, admin:gpg_key, admin:org, admin:org_hook, admin:public_key, admin:repo_hook, admin:ssh_signing_key, audit_log, codespace, copilot, delete:packages, delete_repo, gist, notifications, project, repo, user, workflow, write:discussion, write:network_configurations, write:packages`
- Status: Never used
- Actions: [Configure SSO](#) (dropdown), [Delete](#)

A warning message at the bottom states: **This token has no expiration date.**

A modal window titled 'Single sign-on organizations' is open, showing the following information:

- Header: Configure SSO ▾, Delete
- Section: Single sign-on organizations
- Description: These organizations require tokens to be authorized for access.
- Link: See the documentation for more information.
- Search bar:
- Section: Available to authorize
- Description: Token must be authorized for use in these organizations:

Mutable actions

[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
tj-actions/changed-files (GitHub Actions)	<= 45.0.7	46.0.1

Description
Summary
A supply chain attack compromised the tj-actions/changed-files GitHub Action, impacting over 23,000 repositories. Attackers retroactively modified multiple version tags to reference a malicious commit, exposing CI/CD secrets in workflow logs. The vulnerability existed between March 14 and March 15, 2025 , and has since been mitigated. This poses a significant risk of unauthorized access to sensitive information.
This has been patched in v46.0.1 .
Details
The attack involved modifying the tj-actions/changed-files GitHub Action to execute a malicious Python script. This script extracted secrets from the Runner Worker process memory and printed them in GitHub Actions logs, making them publicly accessible in repositories with public workflow logs.

Severity
High 8.6 / 10
CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	None
Availability	None
Learn more about base metrics	

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

EPSS score
88.385% (99th percentile)

Code Injection

Code scanning alerts / #3

Expression injection in Actions

Fixed in master on Jun 11

.github/workflows/promote.yaml

```
35
36
37
38
39
40
41
42
43
44
```

Potential in: Potential in: CodeQL

albrektsson commented on Jun 5

```
/promote '$(echo $RUNNER_WORKSPACE)'
```

1

github-actions bot commented on Jun 5

```
promote til /home/runner/work/k9-sak feilet
```

Manglet semikolon (#9123)

Verified ✓ 3669a46

First detected in commit on Jun 4

.github/workflows/promote.yaml:38 on branch master

Code scanning alerts / #3

Expression injection in Actions

Fixed in master on Jun 11

.github/workflows/promote.yaml

```
35
36
37
38
39
40
41
42
43
44
```

Potential in: Potential in: CodeQL

albrektsson commented on Jun 5

```
/promote '$(echo $RUNNER_WORKSPACE)'
```

1

github-actions bot commented on Jun 5

```
promote til /home/runner/work/k9-sak feilet
```

Manglet semikolon (#9123)

Verified ✓ 3669a46

First detected in commit on Jun 4

.github/workflows/promote.yaml:38 on branch master

Konfigurasjonen av repo

Branch rules

Restrict creations

Only allow users with bypass permission to create matching refs.

Restrict updates

Only allow users with bypass permission to update matching refs.

Restrict deletions

Only allow users with bypass permissions to delete matching refs.

Require linear history

Prevent merge commits from being pushed to matching refs.

Require deployments to succeed

Choose which environments must be successfully deployed to before refs can be pushed into a ref that matches this rule.

Require signed commits

Commits pushed to matching refs must have verified signatures.

Require a pull request before merging

Require all commits be made to a non-target branch and submitted via a pull request before they can be merged.

Require status checks to pass

Choose which status checks must pass before the ref is updated. When enabled, commits must first be pushed to another ref where the checks pass.

Block force pushes

Prevent users with push access from force pushing to refs.

Require code scanning results

Choose which tools must provide code scanning results before the reference is updated. When configured, code scanning must be enabled and have results for both the commit and the reference being updated.

Konfigurasjonen av repo

Actions permissions

Allow all actions and reusable workflows

Any action or reusable workflow can be used, regardless of who authored it or where it is defined.

Disable actions

The Actions tab is hidden and no workflows can run.

Allow jksolbakken actions and reusable workflows

Any action or reusable workflow defined in a repository within jksolbakken can be used.

Allow jksolbakken, and select non-jksolbakken, actions and reusable workflows

Any action or reusable workflow that matches the specified criteria, plus those defined in a repository within jksolbakken, can be used. [Learn more about allowing specific actions and reusable workflows to run.](#)

Require actions to be pinned to a full-length commit SHA

Konfigurasjonen av repo

Approval for running fork pull request workflows from contributors

Choose which subset of users will require approval before running workflows on their pull requests. Both the pull request author and the actor of the pull request event triggering the workflow will be checked to determine if approval is required. If approval is required, a user with write access to the repository must [approve the pull request workflow to be run](#).

Require approval for first-time contributors who are new to GitHub

Only users who are both new on GitHub and who have never had a commit or pull request merged into this repository will require approval to run workflows.

Require approval for first-time contributors

Only users who have never had a commit or pull request merged into this repository will require approval to run workflows.

Require approval for all external contributors

All users that are not a member or owner of this repository will require approval to run workflows.

Konfigurasjonen av repo

Environments / Configure test

Deployment protection rules

Configure reviewers, timers, and custom rules that must pass before deployments to this environment can proceed.

Required reviewers

Specify people or teams that may approve workflow runs when they access this environment.

Add up to 5 more reviewers

Search for people or teams...



jksolbakken

X

Prevent self-review

Require a different approver than the user who triggered the workflow run.

Wait timer

Set an amount of time to wait before allowing deployments to proceed.

Enable custom rules with GitHub Apps Preview

[Learn about existing apps](#) or [create your own protection rules](#) so you can deploy with confidence.

Allow administrators to bypass configured protection rules

Save protection rules

Deployment branches and tags

Limit which branches and tags can deploy to this environment based on rules or naming patterns.

Selected branches and tags ▾

No branch or tag rules applied yet: **all branches and tags are still allowed to deploy.**

⊕ Add deployment branch or tag rule

Time for arbeidsbutikk!

Forke eller klone amazing-app.

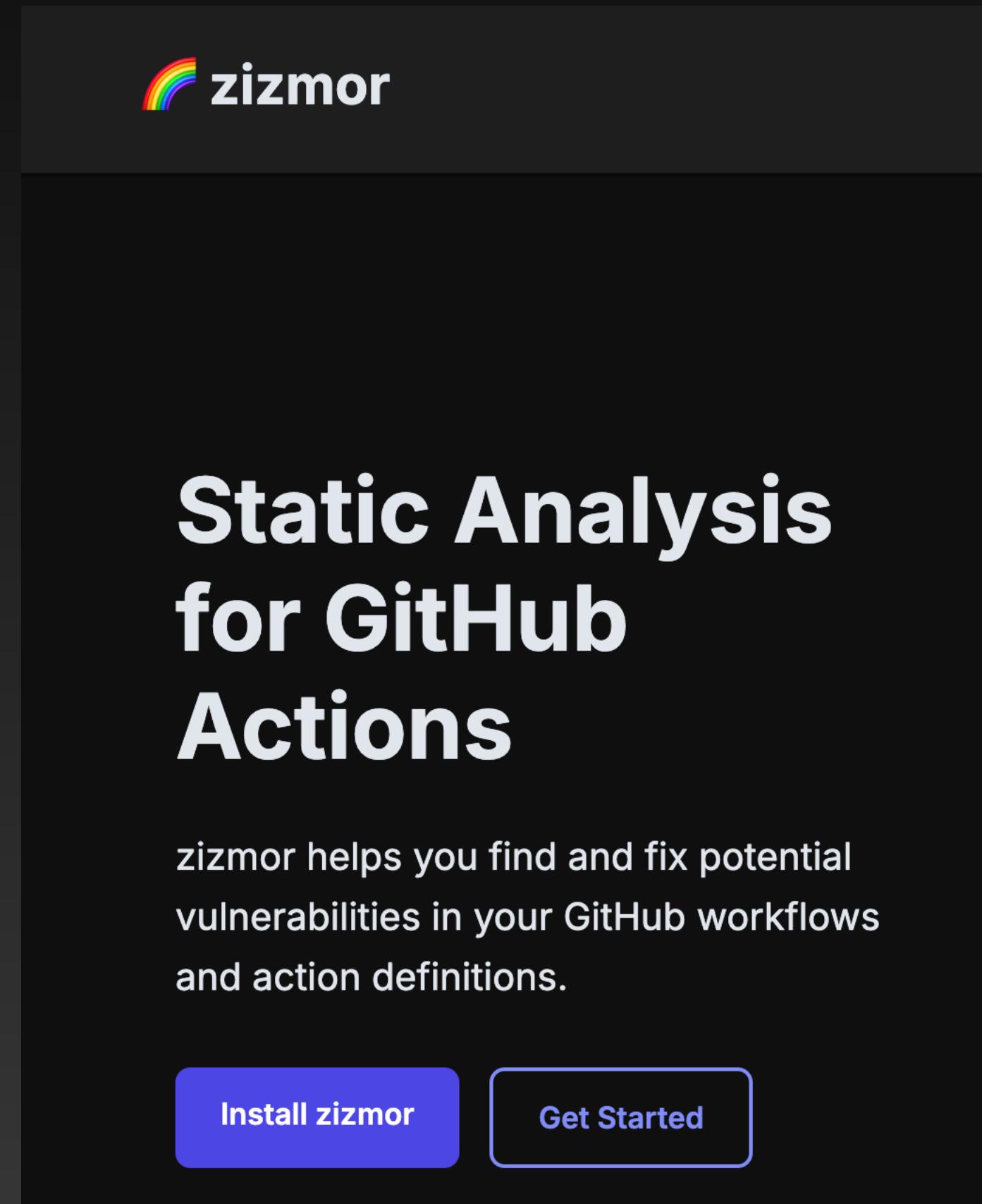
Git clone <https://github.com/CND-Bergen/amazing-app.git>

Gh clone repo CND-Bergen/amazing-app

Bruk 10 min og se om du finner noen sårbarheter i workflowsa her!

Zizmor

<https://zizmor.sh/>



Cache poisoning

Github specific-ish vulnerability

Tl;dr: don't use cache for releases or prod deployment

Bonusoppgaver

Tilbake til amazing-app

Bruk det du har lært til å eksfiltrere hemmeligheter

Finn det hemmelige repoet

Poste en issue med ditt alias > great success!

Thanks for all the phish!

Nyttige linker

- [Preventing pwn requests](#)
- [Security hardening for GitHub Actions](#)
- [How to Harden GitHub Actions: The Unofficial Guide](#)
- [Zizmor](#)
- [Ratchet](#)
- [GitHub token permissions Monitor](#)
- [StepSecurity harden-runner](#)
- [Privesc vha workflow run](#)
- [OpenSSF Scorecard](#)
- [Gato \(Github Attack T0olkit\) - Extreme Edition](#)
- [CodeQL query help for GitHub Actions](#)