مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Supply Chain Compromise in GitHub Action

Tracking #:432316987

Date:19-03-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a significant security incident has been identified involving the popular GitHub Action tj-actions/changed-files, which is widely used in CI/CD pipelines.

## TECHNICAL DETAILS:

A significant security incident has been identified involving the popular GitHub Action **tj-actions/changed-files**, which is widely used in CI/CD pipelines. The attack resulted in the exposure of CI/CD secrets, including AWS access keys, GitHub Personal Access Tokens (PATs), npm tokens, and private RSA keys.

The attack, assigned **CVE-2025-30066** with a CVSS score of 8.6, involved unauthorized modifications to the action's codebase. The attacker(s) retroactively updated multiple version tags to reference a malicious commit, causing sensitive secrets to be printed in GitHub Actions build logs. Organizations utilizing this GitHub Action are at risk of unauthorized access and credential leakage.

The malicious activity was first observed before March 14, 2025, and has since been mitigated. Affected users are strongly advised to take immediate remediation steps to secure their environments.

**Details of the Incident**

- **Impacted Component:** tj-actions/changed-files GitHub Action (used in over 23,000 repositories)
- **CVE Identifier:** CVE-2025-30066
- **CVSS Score:** 8.6 (High)
- **Date of Incident:** Before March 14, 2025
- **Attack Method:**
  - The attacker gained unauthorized access to the repository by compromising a **GitHub Personal Access Token (PAT)** associated with @tj-actions-bot.
  - The attacker modified the codebase and **retroactively updated multiple version tags** to reference a malicious commit.
  - The modified GitHub Action executed a Python script hosted on a GitHub gist (now removed), which extracted CI/CD secrets from the Runner Worker process.
  - If workflow logs were publicly accessible, exposed secrets could have been exploited by unauthorized entities.

**Potential Impact**

- Unauthorized access to CI/CD secrets, including:
  - **AWS access keys**
  - **GitHub Personal Access Tokens (PATs)**
  - **npm tokens**
  - **Private RSA keys**
- Increased risk of **supply chain attacks** affecting software development pipelines.
- Exposure of **sensitive credentials** leading to potential compromise of infrastructure and services.

## RECOMMENDATIONS:

**Immediate Actions:**

- Update to v46.0.1: All users must upgrade to the patched version immediately.

**Review and Revoke Compromised Secrets:**

- Identify all workflows executed between March 14 and March 15, 2025.
- Check for unexpected output under the changed-files section.
- Revoke and regenerate any exposed secrets found in logs.

**Enhance Security Measures:**

- Restrict public access to GitHub Actions workflow logs.
- Implement Principle of Least Privilege (PoLP) for repository access and GitHub Actions.
- Use OpenID Connect (OIDC) authentication instead of PATs for improved security.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-30066