Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

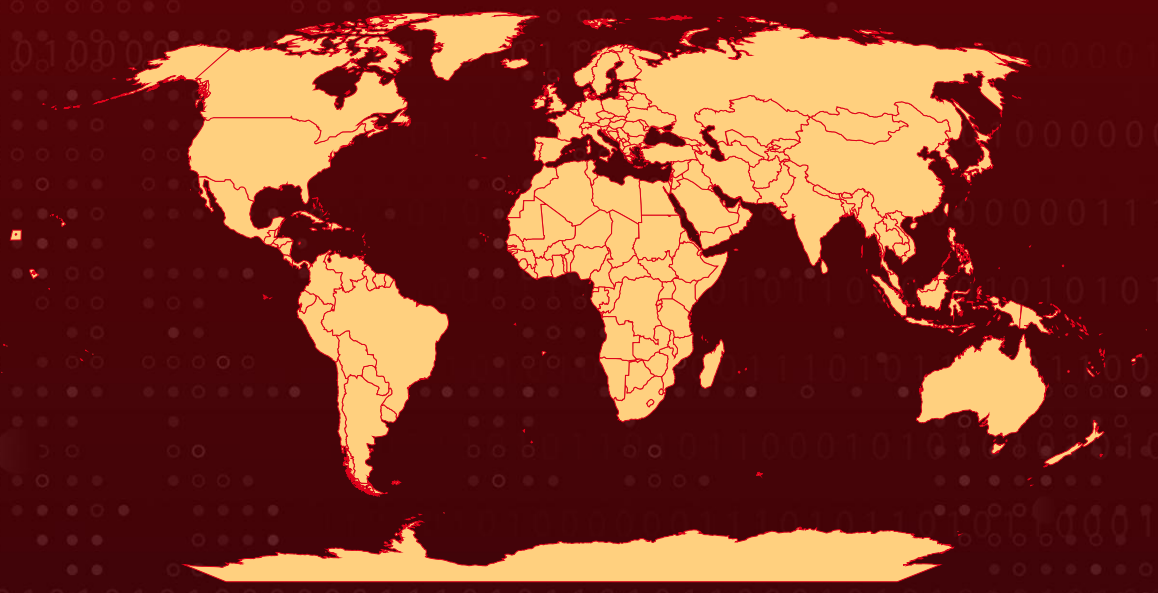
Cascading Supply Chain Attacks in GitHub Actions Exposes CI/CD Secrets

Date of Publication	Admiralty Code	TA Number
March 20, 2025	A1	TA2025085

Summary

Attack Commenced: March 11, 2025
Targeted Countries: Worldwide
Targeted Paltform: GitHub Action
Attack: A recent sophisticated supply chain attack compromised the reviewdog/action-setup@v1 GitHub Action, exposing secrets in CI/CD workflows. The breach, assigned CVE-2025-30154, led to a secondary attack on tj-actions/changed-files (CVE-2025-30066), affecting over 23,000 repositories. Attackers exploited a GitHub Personal Access Token (PAT) to inject malicious code, escalating the impact. Organizations are advised to review logs, rotate secrets, and pin actions to specific commit SHAs to mitigate risks.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-30066	tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability	GitHub Action	✗	✓	✓
CVE-2025-30154	reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability	GitHub Action	✗	✓	✓

Attack Details

#1 A recent sophisticated supply chain attack targeted the reviewdog/action-setup@v1 GitHub Action, leading to the exposure of sensitive information across numerous repositories. GitHub Actions is a CI/CD automation platform that enables developers to automate workflows, such as building, testing, and deploying code, directly within GitHub repositories.

#2 This incident has been assigned the identifier CVE-2025-30154. Attackers injected malicious code into the action's repository, designed to extract secrets from the CI runner's memory and print them in workflow logs. In public repositories, these logs became accessible to anyone, thereby exposing confidential information.

#3 The compromised reviewdog/action-setup action had a cascading effect, leading to the breach of another GitHub Action, tj-actions/changed-files, which is utilized by over ***23,000*** repositories. This subsequent attack has been designated as CVE-2025-30066. Attackers exploited a GitHub Personal Access Token (PAT) associated with a bot account to inject malicious code into this action. This code similarly extracted secrets from CI workflows and exposed them in public logs. The initial compromise of reviewdog/action-setup is believed to have facilitated the theft of the PAT, resulting in the subsequent breach of tj-actions/changed-files.

#4 The exact method by which attackers gained write access to the reviewdog repositories remains under investigation. The reviewdog organization had an automated system that invited contributors and granted them write access for maintaining actions. This system potentially increased the attack surface, allowing unauthorized access either through compromised contributor accounts or malicious actors exploiting the automated invitations. In response, the reviewdog team disabled the automated inviter workflow, revoked write access from most contributors, and updated all repositories to specify GitHub Actions by commit SHA explicitly.

#5 The impact of this supply chain attack is substantial, as it compromised multiple GitHub Actions and exposed secrets across numerous repositories. This incident underscores the critical importance of securing CI/CD pipelines and the potential risks associated with third-party dependencies in software development workflows.

Recommendations

Identify and Remove Compromised Actions: Search repositories for references to reviewdog/action-setup@v1 and tj-actions/changed-files. Immediately remove or replace affected actions with verified alternatives.

Review Workflow Logs for Anomalies: Check past workflow runs for unusual activity, such as unexpected logs containing base64-encoded secrets. Investigate any unauthorized access or modifications in repositories using these actions.

Rotate Exposed Secrets: Revoke and regenerate GitHub secrets, API tokens, and any other credentials potentially exposed in workflow logs. Update environment variables and repository secrets to prevent further exploitation.

Pin GitHub Actions to Specific Commit SHAs: Instead of using mutable tags (e.g., @v1 or @latest), specify fixed commit SHAs to prevent unauthorized updates. Regularly verify the integrity of third-party GitHub Actions before updating.

Restrict Third-Party Actions: Configure repository settings to allow only trusted GitHub Actions. Use GitHub's allowed-actions policy to limit external actions to an approved list.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control
TA0040 Impact	T1195 Supply Chain Compromise	T1098 Account Manipulation	T1078 Valid Accounts
T1027 Obfuscated Files or Information	T1552.001 Credentials In Files	T1552 Unsecured Credentials	T1059 Command and Scripting Interpreter
T1041 Exfiltration Over C2 Channel	T1068 Exploitation for Privilege Escalation	T1195.002 Compromise Software Supply Chain	

Patch Details

CVE-2025-30066: Update tj-actions/changed-files to version 46.0.1.
CVE-2025-30154: Update reviewdog/action-setup@v1 to version v1.3.2.

Links:
https://github.com/tj-actions/changed-files/releases/tag/v46.0.1

https://github.com/reviewdog/action-setup/releases/tag/v1.3.2

References

https://www.wiz.io/blog/new-github-action-supply-chain-attack-reviewdog-action-setup

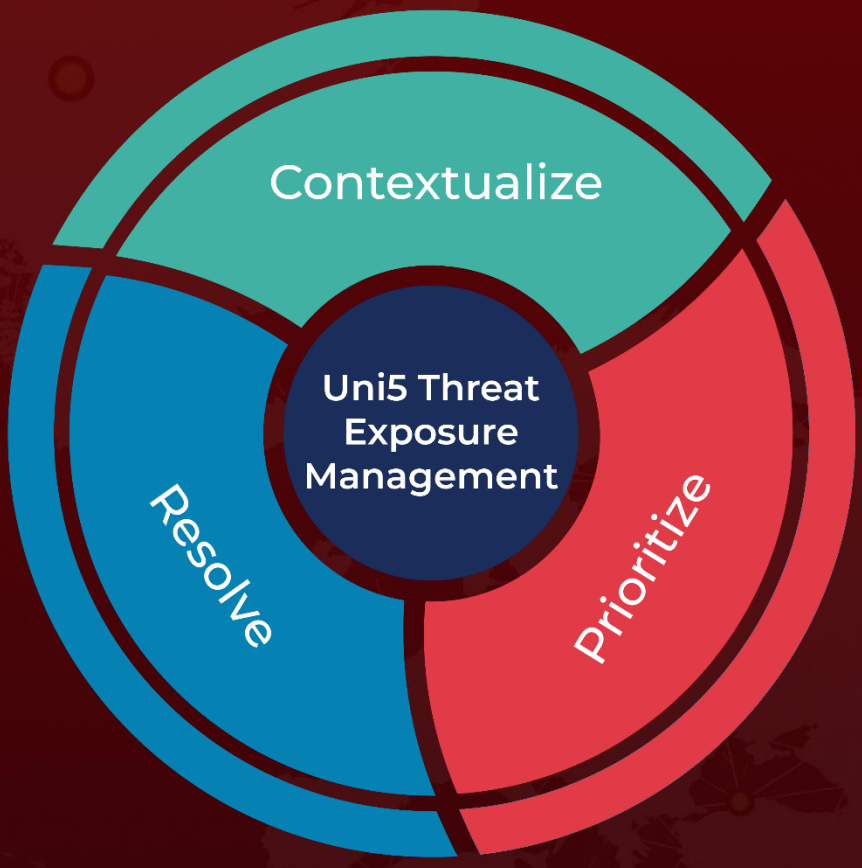
https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-github-action-cve-2025-30066

https://github.com/reviewdog/reviewdog/security/advisories/GHSA-qmg3-hpqr-gqvc

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 20, 2025 • 3:30 AM

More at www.hivepro.com