

CVE-2025-30154

reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability

CISA KEV since Mar 24, 2025

Actively exploited

reviewdog/action-setup is a GitHub action that installs reviewdog. reviewdog/action-setup@v1 was compromised March 11, 2025, between 18:42 and 20:31 UTC, with malicious code added that dumps exposed secrets to Github Actions Workflow Logs. Other reviewdog actions that use `reviewdog/action-setup@v1` that would also be compromised, regardless of version or pinning method, are reviewdog/action-shellcheck, reviewdog/action-composite-template, reviewdog/action-staticcheck, reviewdog/action-ast-grep, and reviewdog/action-typos.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.6 High · NVD	EPSS 0.025 84.5th percentile · FIRST	CISA DEADLINE Apr 14, 2025 KEV since 2025 · listed over a year
--	---------------------------------------	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.025 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.6	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations as set forth in the CISA instructions linked below. Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source project, third-party library, or a protocol used by different products. For more information, please see: CISA Mitigation Instructions: <https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-tj-actionschanged-files-cve-2025-30066-and-reviewdogaction>
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
reviewdog/action-setup	= 1	no fixed version listed	GitHub
action-ast-grep	< 1.26.2	1.26.2	NVD
action-composite-template	< 0.20.2	0.20.2	NVD
action-setup	1	no fixed version listed	NVD
action-shellcheck	< 1.29.2	1.29.2	NVD
action-staticcheck	< 1.26.2	1.26.2	NVD
action-typos	< 1.17.2	1.17.2	NVD



Sources

Vendor guidance	github.com/reviewdog/action-setup/commit/3f401fe1d58fe77e10d665ab713057375e39b887	Additional guidance	github.com/reviewdog/reviewdog/issues/2079
Additional References	github.com/reviewdog/reviewdog/security/advisories/GHSA-qmg3-hpqr-gqvc	NVD	nvd.nist.gov/vuln/detail/CVE-2025-30154
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-qmg3-hpqr-gqvc
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-6724	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-30154

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.