Credential-stealing GitHub Actions workflow pushed to 340+ repositories via hijacked maintainer accounts



Researchers report an ongoing campaign that used two compromised open-source maintainer accounts to push a credential-stealing workflow into more than 340 GitHub repositories. Teams should review their workflows and secrets.

- The campaign is described as ongoing and aimed at stealing credentials.
- Two high-profile open-source maintainer accounts were compromised.
- A malicious workflow was pushed into more than 340 repositories.
- One account belongs to the author of the pyxel game engine, which has 18,400 stars; 27 repositories were hit from 13:20 UTC.
- StepSecurity is the researcher cited in the report.

Researchers have disclosed an ongoing credential-theft campaign that abuses GitHub Actions. According to the report, attackers compromised two high-profile open-source maintainer accounts and used them to push a malicious workflow into more than 340 repositories.

What was observed

StepSecurity reported that one of the accounts belongs to Takashi Kitao, author of the pyxel game engine, which has 18,400 stars. Using that account, the attacker pushed the malicious workflow to 27 repositories starting at 13:20 UTC. The aim of the workflow is to steal credentials. The source headline points to a much larger scale, while the details quoted describe more than 340 repositories, so the full extent should be treated as still emerging.

Why it matters

Workflows run with access to a repository's build environment, and that environment often holds tokens and secrets. A workflow added through a trusted maintainer account can look routine in review. Organisations that fork, mirror or depend on affected open-source projects, or that run their own GitHub Actions pipelines, may be exposed if secrets are reachable from those workflows.

The source does not name specific victims beyond the maintainer accounts, and it does not give indicators of compromise in the excerpt available. Follow the StepSecurity publication for updates.

What to do now

1. Search your repositories and forks for workflow files added or changed recently, especially by maintainer accounts, and review them for unexpected network calls or secret access.
2. Rotate tokens and secrets stored in GitHub Actions for any repository that ran a suspicious workflow.
3. Restrict workflow permissions to the minimum and require review for changes under the workflows directory.
4. Enforce MFA and review access on maintainer and service accounts for your organisation's GitHub.
5. Inventory open-source projects your pipelines depend on, and pin third-party actions to reviewed versions.
6. Report any confirmed exposure through your incident process and, where applicable, to NCA and your sector regulator.