'wfx-loot' campaign abuses 4,800 compromised GitHub accounts to steal CI and cloud secrets



Aikido reports a campaign using 4,837 compromised GitHub accounts to probe 61,764 repositories and steal Actions secrets and cloud credentials. Secrets were taken from at least 1,835 targets.

- The campaign began around 12:45 UTC on November 10, using stolen credentials from 4,837 accounts to test write access on 61,764 repositories.
- Pull requests titled 'docs: dependency audit notes' delivered a 1,500-line shell script; 92% of them remain open.
- The script harvests GitHub tokens, AWS, Azure and Google Cloud credentials, developer and AI-service keys, and can exchange OIDC tokens for temporary cloud sessions.
- Aikido confirmed secrets were stolen from at least 1,835 targets; payloads also reached a Packagist

package and two Go module versions through automated publishing.

- Where execution is confirmed, all secrets and cloud roles available to the affected workflows should be treated as compromised and rotated.

Researchers at Aikido have described a campaign named 'wfx-loot' that targets GitHub Actions secrets and cloud credentials. Not every targeted repository ran the payload, but secrets were stolen from at least 1,835 targets.

How the attack worked

According to Aikido, the attacker used stolen credentials from 4,837 compromised accounts to open pull requests against 61,764 repositories, checking whether each account had write access. The requests were titled 'docs: dependency audit notes'. Some of the compromised accounts reportedly belonged to large organizations and government bodies, and about 50 appear to hold publishing rights on ecosystems such as npm, PyPI, Go, crates and Packagist.

Where access allowed, a shell script of roughly 1,500 lines was delivered by changing an existing workflow, adding a workflow on a short-lived branch, or planting an npm install hook. It collects workflow tokens, cloud credentials for AWS, Azure and Google Cloud, credentials for tools such as Git, SSH, Docker, Kubernetes, Vault and Terraform, and keys for AI services. It can also exchange OIDC tokens for temporary cloud sessions and, where permissions allow, create long-lived credentials or alter identity and trust policies. Data was sent to attacker-controlled endpoints, and changes, workflow runs and logs were removed in under a minute.

What owners should check

Aikido advises repository owners to look for the 'wfx-docs' branch, the probe pull request, and gaps in workflow run numbers. If execution is confirmed, every secret and cloud role available to the affected workflows should be considered compromised and rotated immediately. The researchers believe the main goal was stealing CI secrets, with the package releases a by-product of automated publishing.

What to do now

1. Search your GitHub repositories for the 'wfx-docs' branch, pull requests titled 'docs: dependency audit notes', and unexplained gaps in workflow run numbers.
2. If payload execution is confirmed, rotate all secrets and cloud roles available to the affected workflows immediately, including AWS, Azure, GCP, registry and AI-service keys.
3. Review cloud audit logs for new long-lived IAM credentials, role chaining, or changes to identity and trust policies made from CI identities.
4. Check whether any of your packages or modules were published automatically from affected workflows, and verify the integrity of recent releases.

5. Restrict write access and Actions permissions to the minimum required, and enforce MFA and credential hygiene for developer accounts.