Threat Advisory:

# Aqua Security Trivy GitHub Action Compromised

Status: **Exploited in the Wild**

**Published :** 23/03/2026

RelianceCyber

# Threat Summary.

Security researchers have identified a supply-chain compromise affecting the aquasecurity/trivy-action GitHub action, a widely used vulnerability scanning tool.

Compromised versions point to malicious code which could be used as an information stealer to extract secrets and credentials from an affected system.

In addition, if it detects it is on a developer machine it additionally writes a base64 encoded python dropper for persistence.

Any pipeline that executed an affected action after 19:00 on 19th March 2026 should be considered fully compromised and all secrets should be reset.

For self-hosted GitHub runners, any additional credentials stored on the device's filesystem should be reset.

A detailed writeup can be found here.

# Recommended Actions

Organizations should stop using trivy-action by version tag immediately. The only safe options are pinning to **commit SHA 57a97c7e7821a5776cebc9bb87c984fa69cba8f1** or using **tag 0.35.0 exclusively.**

Any pipeline that executed a poisoned tag should be treated as fully compromised.

All secrets accessible to that workflow including cloud credentials, SSH keys, API tokens, database passwords, docker registry tokens should be rotated immediately.

Security teams should **audit their GitHub** organization for tpcp-docs repositories and review GitHub Actions logs for any trivy-action runs occurring after approximately 19:00 UTC on March 19, 2026.

# What are Reliance Cyber doing?

Reliance Cyber are threat hunting for indicators below :

| Indicator | Notes |
|---|---|
| scan.aquasecurtiy(.)org | Typosquatted C2 |
| 45.148.10(.)212 | TECHOFF SRV LIMITED, Amsterdam |
| tdtqy-oyaaa-aaaae-af2dq-cai.raw.icp0(.)io | ICP-hosted fallback within malicious Trivy binary |
| plug-tab-protective-relay.trycloudflare(.)com | Used within GitHub Actions for exfiltration |
| 887e1f5b5b50162a60bd03b66269e0ae545d0aef0583c1c5b00972152ad7e073 | FreeBSD-64bit |
| f7084b0229dce605ccc5506b14acd4d954a496da4b6134a294844ca8d601970d | Linux-32bit |
| 822dd269ec10459572dfaaefe163dae693c344249a0161953f0d5cdd110bd2a0 | Linux-64bit |
| bef7e2c5a92c4fa4af17791efc1e46311c0f304796f1172fce192f5efc40f5d7 | Linux-ARM |
| e64e152afe2c722d750f10259626f357cdea40420c5eedae37969fbf13abbecf | Linux-ARM64 (unconfirmed) |
| ecce7ae5ffc9f57bb70efd3ea136a2923f701334a8cd47d4fbf01a97fd22859c | Linux-PPC64LE |
| d5edd791021b966fb6af0ace09319ace7b97d6642363ef27b3d5056ca654a94c | Linux-s390x |
| e6310d8a003d7ac101a6b1cd39ff6c6a88ee454b767c1bdce143e04bc1113243 | macOS-64bit |
| 6328a34b26a63423b555a61f89a6a0525a534e9c88584c815d937910f1ddd538 | macOS-ARM64 |
| 0880819ef821cff918960a39c1c1aada55a5593c61c608ea9215da858a86e349 | Windows-64bit |

# Sources

https://digital.nhs.uk/cyber-alerts/2026/cc-4758

https://socket.dev/blog/trivy-under-attack-again-github-actions-compromise

https://www.csoonline.com/article/4148317/trivy-vulnerability-scanner-backdoored-with-credential-stealer-in-supply-chain-attack.html

https://www.aquasec.com/blog/trivy-supply-chain-attack-what-you-need-to-know/

https://www.wiz.io/blog/trivy-compromised-teampcp-supply-chain-attack

https://www.crowdstrike.com/en-us/blog/from-scanner-to-stealer-inside-the-trivy-action-supply-chain-compromise/

https://socket.dev/blog/trivy-under-attack-again-github-actions-compromise

RelianceCyber

+44 020 3872 9000 ☎

contact@reliancecyber.com @

www.reliancecyber.com