AccuKnox

Trivy Supply Chain Compromise

Credential Exfiltration via Malicious GitHub Actions

Issued: March 25, 2026
Updated: March 25, 2026

Severity
CRITICAL

Summary

Active Supply Chain Attack

Threat actor group TeamPCP has compromised the official Trivy release pipeline. Malicious versions v0.69.4 and v0.69.5 are live and actively exfiltrating credentials from affected CI/CD environments.

AccuKnox Infrastructure `[Not Directly Vulnerable]`

Our platform uses a strictly pinned, securely hosted Trivy binary. We do not dynamically pull from public repositories at runtime. Credential rotation is still recommended as a precaution against indirect exposure.

What Happened

Threat actor group TeamPCP compromised the official Trivy release pipeline and injected credential-stealing malware into two specific release versions. The attack also included force-pushing malicious code into the `trivy-action` and `setup-trivy` GitHub Actions.

The malware scrapes environment memory and file systems on execution, exfiltrating SSH keys, cloud credentials, and Kubernetes service account tokens to attacker-controlled infrastructure.

This is a confirmed active attack. Any CI/CD pipeline that referenced Trivy by mutable tag or downloaded from the official release pipeline without hash pinning is at risk.

Trivy Component Versions

Threat actor group TeamPCP compromised the official Trivy release pipeline and injected credential-stealing malware into two specific release versions. The attack also included force-pushing malicious code into the trivy-action and setup-trivy GitHub Actions.

Version	Status	Notes
`v0.69.4`	VULNERABLE	Malicious binary injected into release pipeline
`v0.69.5`	VULNERABLE	Malicious binary injected into release pipeline
`v0.69.3 and earlier`	NOT AFFECTED	Pipeline was not compromised before v0.69.4
`trivy-action (all)`	VULNERABLE	Force-pushed malicious code to GitHub Actions
`setup-trivy (all)`	VULNERABLE	Force-pushed malicious code to GitHub Actions

Where AccuKnox Uses Trivy

The following surfaces integrate Trivy within the AccuKnox platform. Each has been assessed for direct and indirect exposure.

🟢	In-cluster scanning	Not affected — pinned binary
🟢	Image registry scanning	Not affected — pinned binary
🟢	CI/CD pipeline integrations	Not affected — no trivy-action usage
🟢	ASPM CLI tool	Not affected — bundled pinned binary
🟡	Custom team pipelines	Audit required

If your team uses Trivy independently — outside AccuKnox-managed workflows — your custom pipelines may still be at risk. See Section 4 for immediate steps.

Recommended Actions

01	Rotate all GitHub Secrets and Personal Access Tokens (PATs). Treat them as compromised if any pipeline ran Trivy v0.69.4 or v0.69.5.
02	Audit your pipelines for any direct use of trivy-action or setup-trivy. Replace with a pinned, hash-verified binary from a trusted mirror.
03	Check for Trivy v0.69.4 or v0.69.5 in any pipeline — Docker image, shell script download, or GitHub Actions reference.
04	Rotate cloud credentials (AWS, GCP, Azure) and Kubernetes service account tokens as a precaution, particularly if shared environments exist between development and CI/CD.
05	Run the AccuKnox IOC Scanner CLI to check local environments, container images, and CI/CD workflows for Indicators of Compromise tied to this breach.

IOC Scanner CLI

```
# AccuKnox IOC Scanner — scan for Trivy supply chain IOCs
gh extension install accuknox/gh-audit --branch trivy
gh accuknox audit --scan-mode=trivy-ioc --output=report.json
```

IOC Scanner repo: github.com/accuknox/gh-audit/tree/trivy — Questions? Contact support@accuknox.com.

Timeline (UTC)

2026-03-24 ~18:00	TeamPCP supply chain compromise of Trivy release pipeline first observed by external researchers.
2026-03-25 08:00	AccuKnox Security team begins internal impact assessment across all product integrations.
2026-03-25 11:30	AccuKnox infrastructure confirmed not directly vulnerable — pinned binary architecture validated.

2026-03-25 14:00	IOC Scanner CLI deployed to GitHub at accuknox/gh-audit/tree/trivy.
2026-03-25 16:00	This advisory was issued to customers. Credential rotation guidance published.
Ongoing	Monitoring for further upstream developments. Advisory will be updated as new information becomes available.

References

1. Full technical breakdown including attack mechanics and specific IOC hashes: Wiz Threat Research Report
2. AccuKnox IOC Scanner CLI: github.com/accuknox/gh-audit/tree/trivy
3. OWASP Vulnerability Disclosure Cheat Sheet: cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html