مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

# Critical Supply Chain Compromise in Trivy Ecosystem

Tracking #:432318667

Date:27-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical software supply chain attack impacted the Aqua Security Trivy ecosystem in March 2026. Threat actors leveraged compromised credentials to distribute malicious versions of Trivy binaries, GitHub Actions, and container images.

## TECHNICAL DETAILS:

A critical software supply chain attack impacted the Aqua Security Trivy ecosystem in March 2026. Threat actors leveraged compromised credentials to distribute malicious versions of Trivy binaries, GitHub Actions, and container images.

The attack stems from incomplete (non-atomic) credential rotation following an earlier breach disclosed on March 1, 2026. This gap enabled attackers to maintain persistence and execute a second-stage attack on March 19, introducing credential-stealing malware into widely used CI/CD components.

This vulnerability has been assigned a CVSS 4.0 score of 9.4 (Critical) and is categorized under CWE-506: Embedded Malicious Code, posing a severe risk of secret exfiltration, CI/CD compromise, and downstream supply chain attacks.

### Attack Timeline

- Late February 2026 – Initial supply chain compromise begins
- March 1, 2026 – Initial disclosure and credential rotation (non-atomic)
- March 19, 2026 – Malicious releases and tag tampering conducted
- March 22, 2026 – Additional malicious Docker images (v0.69.5, v0.69.6) published

### Technical Breakdown

- Threat actor used compromised credentials/tokens
- Exploited credential rotation window (lasting several days)
- Inserted credential-stealing malware into:
  - GitHub Actions
  - CLI binaries
  - Container images
- Leveraged force-push attacks on version tags, impacting trust in versioning

### Malicious Activity Observed

- Replacement of legitimate code with credential harvesting logic
- Potential exfiltration of secrets from CI/CD pipelines
- Creation of suspicious repositories such as:
  - tpcp-docs (indicator of successful exfiltration fallback)
- Abuse of mutable version tags instead of immutable commit SHAs

### Vulnerability Classification

- CVE-2026-33634
- CWE:
  - CWE-506 – Embedded Malicious Code

- CVSS v4.0:
    - Score: 9.4 (Critical)
    - Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H

**Impact Assessment**
Organizations using affected versions may face:

- Full CI/CD pipeline compromise
- Exposure of secrets, including:
    - API keys
    - Cloud credentials
    - Tokens
- Lateral movement into production environments
- Downstream supply chain compromise

## RECOMMENDATIONS:

1. **Identify Exposure**
    - Check for usage of:
        - Trivy 0.69.4,0.69.5 and v0.69.6 (or latest during the exposure window) distributed via Docker Hub.
        - Compromised GitHub Actions versions
2. Update to Known-Safe Versions
3. **Remove Malicious Artifacts**
    - Delete affected binaries, images, and cached layers
4. **Rotate All Secrets**
    - Treat all CI/CD-accessible secrets as compromised
    - Rotate:
        - GitHub tokens
        - Cloud credentials
        - API keys

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23