INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:34 UTC

# TeamPCP Supply Chain Campaign Compromises Developer Security Toolchain: KICS, Trivy, VS Code, and LiteLLM

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0100 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | Checkmarx KICS (GitHub Action), Trivy, VS Code plugins (unspecified), LiteLLM AI library |
| **Published** | 2026-03-24 |
| **Discovery Source** | Rss |

## Executive Summary

A threat actor tracked as TeamPCP has conducted a coordinated supply chain attack against multiple developer and security tools used widely in enterprise DevSecOps pipelines, including Checkmarx KICS, Trivy, VS Code extensions, and the LiteLLM AI library. The attack targets upstream components such as GitHub Actions and open-source package repositories, injecting malicious code into tooling that runs with elevated trust during builds, scans, and code development. Organizations using any of these tools in automated pipelines face risk of backdoor installation, credential theft, and downstream compromise of production environments, with activity assessed as ongoing by multiple vendors.

## Technical Analysis

TeamPCP is executing a multi-vector software supply chain campaign mapped to MITRE ATT&CK techniques T1195.001 (Compromise Software Dependencies and Development Tools), T1195.002 (Compromise Software Supply Chain), T1554 (Compromise Client Software Binary), T1072 (Software Deployment Tools), T1078.004 (Cloud Accounts), T1566.003 (Spearphishing via Service), and T1059 (Command and Scripting Interpreter). The attack chain involves compromising upstream GitHub Actions and open-source packages to inject malicious code into: Checkmarx KICS GitHub Action (static analysis), Trivy (container and filesystem vulnerability scanner), unspecified VS Code IDE extensions, and the LiteLLM AI inference library. Malicious code injected into these tools executes within CI/CD pipelines and developer workstations at a high-trust level, enabling persistence, lateral movement, and data exfiltration. CWE mapping: CWE-494 (Download of Code Without Integrity Check), CWE-829 (Inclusion of Functionality from Untrusted Control Sphere), CWE-506 (Embedded

Malicious Code). No CVE has been assigned. Specific compromised versions have not been consolidated into a single advisory; vendors Wiz, Endor Labs, Snyk, and ReversingLabs have each published technical findings. Activity is assessed as ongoing beyond the initial KICS disclosure per Endor Labs and ReversingLabs technical findings.

## Action Checklist

1. Step 1, Immediate: Pin or freeze all GitHub Actions references to a known-good commit SHA rather than a mutable tag; audit any pipeline using the KICS GitHub Action, Trivy, or LiteLLM for recent unexpected changes to workflow files or dependency manifests.
2. Step 2, Immediate: Review VS Code extension inventory across developer endpoints; remove or disable extensions installed from unverified publishers or recently updated without a corresponding changelog entry.
3. Step 3, Detection: Search CI/CD pipeline logs for unexpected outbound network connections, process spawns, or file writes originating from KICS, Trivy, or LiteLLM execution steps; look for base64-encoded commands or curl/wget invocations within scanner output.
4. Step 4, Assessment: Inventory all pipelines and developer workstations that executed a potentially affected version of KICS GitHub Action, Trivy, or LiteLLM within the past 90 days; treat any secrets or credentials accessible during those runs as potentially compromised.
5. Step 5, Communication: Notify application security, DevOps, and platform engineering teams of the campaign scope; escalate to incident response if pipeline compromise is confirmed or if credential exposure cannot be ruled out.
6. Step 6, Long-term: Implement or enforce a software supply chain integrity policy requiring cryptographic verification (e.g., Sigstore/cosign for container images, artifact signing for GitHub Actions) and establish a recurring audit cycle for third-party CI/CD dependencies and IDE extensions.

## Detection Guidance

Detection should focus on three layers. Pipeline layer: inspect CI/CD logs for scanner steps (KICS, Trivy) spawning child processes outside their expected execution tree, making outbound connections to non-vendor infrastructure, or writing files outside designated output directories. Query example (GitHub Actions log pattern): search runner logs for process names kics, trivy, or litellm followed by curl, wget, python -c, or base64 within the same job run. Endpoint layer: on developer workstations, monitor VS Code extension host processes (extensionHost) for unexpected network connections or file system writes to credential stores (e.g., ~/.ssh, ~/.aws, OS keychain paths). Dependency layer: compare current lockfile hashes (package-lock.json, requirements.txt, go.sum) against a baseline from before the suspected compromise window; flag any LiteLLM or Trivy dependency that changed without a corresponding pull request. Behavioral IOC: outbound DNS or HTTP requests to infrastructure not associated with Checkmarx, Aqua Security, or LiteLLM official domains originating from scanner or AI library process contexts should be treated as high-confidence indicators of compromise pending investigation. Specific IOC values (IPs, domains, hashes) have not been independently verified for this response and are not included; consult the Wiz, ReversingLabs, Endor Labs, and Snyk technical reports directly for confirmed IOC lists.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `https://www.wiz.io/blog/teampcp-attack-kics-github-action` | Wiz technical report — primary source for KICS GitHub Action compromise details and potential IOC list | HIGH |
| URL | `https://www.reversinglabs.com/blog/teampcp-supply-chain-attack-spreads` | ReversingLabs report covering LiteLLM compromise and ongoing TeamPCP activity | HIGH |
| URL | `https://www.endorlabs.com/learn/teampcp-isnt-done` | Endor Labs report confirming actor operations continue beyond KICS initial disclosure and covering Trivy | HIGH |
| URL | `https://snyk.io/articles/poisoned-security-scanner-backdooring-litellm/` | Snyk technical analysis of LiteLLM backdoor via poisoned security scanner | HIGH |

## Framework Mappings

### MITRE-ATTACK

- **T1072** — Software Deployment Tools
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1078.004** — Cloud Accounts
- **T1566.003** — Spearphishing via Service
- **T1195.002** — Compromise Software Supply Chain
- **T1554** — Compromise Host Software Binary
- **T1059** — Command and Scripting Interpreter

### NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan

### OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

### CIS-V8

- **2.5**
- **2.6**
- **15.1** — Establish and Maintain an Inventory of Service Providers

**ISO-27001-2022**

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

**NIST-CSF-2**

- **GV.SC-01** — Cybersecurity supply chain risk management program

**SOC2-TSC**

- **CC9.2** — Manages risks associated with vendors and business partners

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1072 | Software Deployment Tools | Execution |
| T1195.001 | Compromise Software Dependencies and Development Tools | Initial-Access |
| T1078.004 | Cloud Accounts | Defense-Evasion |
| T1566.003 | Spearphishing via Service | Initial-Access |
| T1195.002 | Compromise Software Supply Chain | Initial-Access |
| T1554 | Compromise Host Software Binary | Persistence |
| T1059 | Command and Scripting Interpreter | Execution |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.darkreading.com/application-security/checkmarx-kics-cod... | T3 |
| **KICS GitHub Action Compromised: TeamPCP Supply Chain Attack** | https://www.wiz.io/blog/teampcp-attack-kics-github-action | T3 |
| **TeamPCP Isn't Done: Threat Actor Behind Trivy and KICS ...** | https://www.endorlabs.com/learn/teampcp-isnt-done | T3 |

| Source | URL | Tier |
|---|---|---|
| **How a Poisoned Security Scanner Became the Key to Backdooring ...** | https://snyk.io/articles/poisoned-security-scanner-backdooring-lite... | T3 |
| **TeamPCP software supply chain attack spreads to LiteLLM** | https://www.reversinglabs.com/blog/teampcp-supply-chain-attack-spreads | T3 |



Generated 2026-03-29 18:34 UTC by TJS Security Command Center