INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-08 18:47 UTC

Trivy Weaponized: TeamPCP (UNC6780) Turns DevSecOps Scanner Into Supply Chain Entry Point, Steals Cisco Source Code

THREAT CAMPAIGN | CRITICAL | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0157
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Cisco (confirmed source code exfiltration); Trivy open-source security scanner (weaponized as attack vector); CI/CD pipeline tooling broadly
Published	2026-04-08T13:15:05
Discovery Source	Rss

Executive Summary

A threat actor tracked as TeamPCP by SANS ISC and UNC6780 by Google GTIG has exploited the Trivy open-source security scanner to compromise CI/CD pipelines, resulting in confirmed Cisco source code theft. The campaign is actively tracked in SANS ISC reporting, inverts a core DevSecOps assumption: that security tooling itself is trustworthy. Defenders should prioritize audit of scanner credentials and pipeline permissions immediately.

Technical Analysis

The TeamPCP campaign represents a deliberate targeting of the security toolchain itself. Trivy, an open-source vulnerability scanner widely deployed in Kubernetes and container CI/CD environments, served as the attack vector rather than the defense. This is a meaningful tactical evolution: attackers are now mapping the tooling organizations trust implicitly and weaponizing it. Security scanners typically run with elevated access to container registries, source code repositories, and secrets stores. Compromising the scanner means compromising everything the scanner can reach. The specific mechanism by which Trivy was exploited has not been fully disclosed in available public reporting as of this analysis; organizations should monitor the SANS ISC Diary for technical indicator updates.

Cisco source code theft is the highest-confidence confirmed impact in available reporting. Supply chain theft of vendor source code carries second-order risk beyond the immediate victim: if adversaries analyze Cisco source code for previously unknown vulnerabilities, downstream customers across enterprise networking and security

infrastructure become potential future targets. Google GTIG's formal tracking of this group as UNC6780 signals that the campaign has met the evidentiary threshold for a distinct threat actor designation, a meaningful indicator of campaign scale and sophistication.

The CI/CD pipeline compromise angle is technically significant. Pipelines often inherit secrets, tokens, and credentials scoped broadly for automation purposes. An attacker who can inject into or manipulate a pipeline stage, particularly one involving a security scanning tool, gains access to artifacts, registries, and potentially signing keys without triggering conventional endpoint or network detections. Organizations running Trivy in automated pipelines should treat any Trivy execution environment as a potential lateral movement surface and audit what credentials and registries it can access.

One structural gap in current reporting is the absence of specific CVE identifiers tied to the Trivy exploitation mechanism. The campaign is confirmed and actively tracked, but the precise vulnerability class used to weaponize Trivy has not been publicly disclosed. This limits the ability to write precise detection rules or apply targeted patches. Until CVEs are published, defenders should focus on behavioral controls: monitoring for anomalous Trivy process behavior, auditing CI/CD pipeline permissions, rotating credentials accessible to scanner tooling, and reviewing pipeline logs for unexpected network connections or artifact access patterns.

Action Checklist

1. Audit Trivy deployment permissions immediately: determine what credentials, registries, and repositories your Trivy instances can access, and apply least-privilege scoping. Scanner tools do not need write access or broad secret access to function.
2. Treat CI/CD pipeline stages running security tooling as high-value lateral movement targets: review pipeline logs for anomalous process execution, unexpected outbound connections, or access to artifacts outside normal scan scope.
3. If your organization uses Cisco networking or security products, monitor Cisco's security advisories and PSIRT disclosures for new CVEs. Source code theft is often a precursor to novel vulnerability discovery targeting downstream customers.
4. Cross-reference IOCs from the SANS ISC Diary against your SIEM and EDR telemetry: the campaign is confirmed active and indicators should be treated as live, not historical.
5. Document use of SANS ISC and Google GTIG reporting as your authoritative source where CISA guidance is not available. This protects your audit posture in compliance review.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if any Trivy instance is confirmed to have executed with access to source code repositories, container image signing keys, cloud provider credentials, or secrets management systems (HashiCorp Vault, AWS Secrets Manager), as this constitutes a confirmed supply chain compromise with potential for downstream customer impact and regulatory breach notification obligations under GDPR, CCPA, or sector-specific frameworks.

Recovery Notes	Before restoring any Trivy instances to production CI/CD pipelines, verify the container image digest or binary hash of every Trivy deployment against the official Aqua Security release hashes published at the official Trivy GitHub releases page — do not trust cached or locally stored images as UNC6780 weaponized the scanner binary itself. Rotate all credentials, tokens, and secrets that were accessible to Trivy execution contexts during the compromise window, including CI/CD platform tokens, container registry credentials, source code repository access tokens, and any cloud IAM roles bound to pipeline service accounts. Monitor CI/CD pipeline execution telemetry and outbound network connections from runner hosts for a minimum of 30 days post-recovery, given the campaign's confirmed active status through April 8, 2026, and the likelihood of persistence mechanisms planted during the access window.
Forensic Artifacts	Trivy binary or container image hash: compare SHA-256 of deployed Trivy binary or image digest against official Aqua Security release hashes — a mismatch is definitive evidence of binary tampering by UNC6780 | CI/CD pipeline job execution logs showing Trivy invocation arguments, stdout/stderr output, and process exit codes for all runs in the 90-day window prior to detection — anomalous flags, unexpected scan targets, or output redirections indicate weaponized execution | Network flow logs and DNS query logs from pipeline runner hosts scoped to Trivy process execution windows — UNC6780 C2 exfiltration of source code would appear as anomalous outbound connections to non-standard destinations during or immediately after Trivy scan stages | Container registry access logs and source code repository audit logs (GitHub audit log, GitLab audit events, Bitbucket audit log) for read/clone events initiated by Trivy service accounts or pipeline tokens outside normal scan scope — these capture the Cisco-style source code exfiltration path | Secrets manager and credential store access logs (AWS CloudTrail GetSecretValue events, HashiCorp Vault audit log, Kubernetes secret access audit events) for any reads performed by Trivy service account identities — confirms whether the weaponized scanner harvested credentials beyond its intended scan function

Per-Action IR Details

Audit Trivy deployment permissions immediately: determine what credentials, registries, and repositories your Trivy instances can access, and apply least-privilege scoping — scanner tools do not need write access or broad secret access to function

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Restrict scope of compromise by limiting attacker-accessible resources before full eradication is complete

Controls: NIST IR-4 (Incident Handling), NIST AC-6 (Least Privilege) — enforce minimum necessary access for Trivy service accounts and pipeline tokens, NIST CM-7 (Least Functionality) — disable Trivy access to secret stores, container registries, and source repos beyond scan targets, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process)

Compensating: Run: `grep -rE '(TRIVY|trivy)' ~/.docker/config.json /etc/environment /home/*/.bashrc /home/*/.profile /etc/profile.d/* 2>/dev/null` to enumerate credential exposure. On Kubernetes: `kubectl get serviceaccounts -A | grep -i trivy` then `kubectl describe serviceaccount -n ` to enumerate bound RBAC roles. Immediately revoke any Trivy service account tokens with `kubectl delete secret ` and reissue scoped-down replacements. For GitHub Actions/GitLab CI: audit `GITHUB_TOKEN` permissions in workflow YAML files for `contents: write` or `packages: write` scopes that Trivy jobs should not require.

Evidence: BEFORE revoking credentials, capture the full permission scope: export `kubectl auth can-i --list --as=system:serviceaccount::` output for each Trivy service account. Snapshot CI/CD environment variable configurations (GitHub Actions secrets list, GitLab CI/CD variables, Jenkins credentials store) to document what secrets were accessible to the Trivy execution context. Preserve container image digests of Trivy versions currently deployed — UNC6780 weaponized the scanner binary itself, so the running image hash is critical forensic evidence of

whether a tampered version was in use.

Treat CI/CD pipeline stages running security tooling as high-value lateral movement targets: review pipeline logs for anomalous process execution, unexpected outbound connections, or access to artifacts outside normal scan scope

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate pipeline telemetry to distinguish legitimate scanner behavior from UNC6780 lateral movement through the DevSecOps toolchain

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: On pipeline runner hosts (GitHub Actions self-hosted, GitLab Runner, Jenkins agent), deploy Sysmon with the SwiftOnSecurity config and specifically enable Event ID 1 (Process Create), Event ID 3 (Network Connect), and Event ID 11 (File Create). Query for: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 3 -and $_.Message -match 'trivy'}` to surface outbound connections initiated by Trivy processes. For Linux runners, use `auditd` with rule: `-a always,exit -F exe=/usr/local/bin/trivy -S connect -k trivy_outbound` and review `/var/log/audit/audit.log` for unexpected destination IPs. Cross-reference Trivy process network destinations against the SANS ISC Diary IOC list for UNC6780 C2 infrastructure.

Evidence: Capture pipeline execution logs for all Trivy job runs in the 90 days preceding detection — specifically the stdout/stderr of Trivy scan invocations, which may reveal unexpected flags, targets, or output destinations injected by UNC6780. Collect runner host process trees: on Linux `ps auxf` snapshots or `/proc/[pid]/cmdline` for Trivy PIDs. Preserve network flow logs (VPC flow logs, NetFlow, or `ss -tnp` snapshots) from runner hosts showing all outbound connections made during Trivy execution windows. For containerized runners, export Docker daemon logs (`journalctl -u docker`) and any `docker inspect` output for the Trivy container showing mounted volumes and environment variables.

If your organization uses Cisco networking or security products, monitor Cisco's security advisories and PSIRT disclosures for new CVEs — source code theft is often a precursor to novel vulnerability discovery targeting downstream customers

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Intelligence sharing and threat-informed posture improvement following confirmed source code exfiltration by UNC6780

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment) — reassess risk posture for Cisco-dependent systems given confirmed source code exposure, NIST IR-8 (Incident Response Plan) — update IR plan to include monitoring cadence for Cisco PSIRT as a standing post-incident action, CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Subscribe to Cisco PSIRT RSS feed at `https://tools.cisco.com/security/center/psirtrss20/CiscoSecurityAdvisory.xml` and pipe new entries into a local alerting script: `curl -s | python3 -c "import sys,xml.etree.ElementTree as ET; [print(i.find('title').text) for i in ET.parse(sys.stdin).findall('.//{*}item')]"`. Set a weekly cron job to diff the advisory list and alert on new critical/high entries. For Cisco IOS/IOS-XE: run `show version` and `show inventory` across your fleet and map installed versions to the Cisco Software Checker tool to pre-identify exposure when novel CVEs emerge from the stolen source code.

Evidence: Document current Cisco product and version inventory (IOS, IOS-XE, NX-OS, ASA, FTD, ISE version strings) NOW as a pre-exposure baseline — this becomes the reference point for rapid impact assessment when UNC6780-derived CVEs surface. Preserve Cisco device configuration exports (`show running-config` or Cisco DNA Center exports) to support rapid diff analysis if a post-source-code-theft vulnerability targets specific configuration patterns. Archive the current Cisco PSIRT advisory index as a dated snapshot to measure new advisory velocity — an unusual spike in Cisco CVEs in coming months is a direct indicator of weaponized source code use.

Cross-reference IOCs from the SANS ISC Diary against your SIEM and EDR telemetry: the campaign is confirmed active as of April 8, 2026, and indicators should be treated as live, not historical

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Prioritize IOC matching against live telemetry given confirmed active campaign status; treat UNC6780 indicators as current threat intelligence, not archived artifacts

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Extract IP, domain, hash, and URI IOCs from the SANS ISC Diary entries for TeamPCP/UNC6780 and operationalize them immediately without a SIEM: (1) Hash IOCs — run `find / -type f -exec md5sum {} \; 2>/dev/null | grep -Ff ioc_hashes.txt` or use `yara -r teamPCP_rules.yar /path/to/scan`; (2) Network IOCs — query DNS resolver logs with `grep -Ff ioc_domains.txt /var/log/named/queries.log` or pfSense/OPNsense firewall logs; (3) IP IOCs — `grep -Ff ioc_ips.txt /var/log/ufw.log` or equivalent host firewall log; (4) For pipeline-specific IOCs, search GitHub Actions workflow run logs and GitLab CI job traces using the IOC list as search strings. Write Sigma rules targeting Trivy process ancestry and outbound connection patterns for use with `sigma convert` against local log files.

Evidence: Before bulk IOC sweeping, preserve unmodified copies of all CI/CD pipeline job logs, runner host syslogs, and network flow data covering the 90 days prior to April 8, 2026 — this is the confirmed active window. Capture DNS query logs from your resolver for all domains resolved by pipeline runner hosts, as UNC6780 C2 communication from weaponized Trivy would appear here. Preserve EDR process execution telemetry or Sysmon Event ID 1 logs for Trivy binary executions, including full command-line arguments and parent process context, as IOC matching against these may reveal the specific campaign variant active in your environment.

Document use of SANS ISC and Google GTIG reporting as your authoritative source for KEV-related compliance requirements where CISA has not issued a standalone advisory — this protects your audit posture if the deadline gap is scrutinized

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Maintain defensible documentation of intelligence sourcing and compliance decision rationale when primary regulatory guidance (CISA KEV advisory) is absent

Controls: NIST IR-6 (Incident Reporting) — document the gap between KEV deadline and CISA advisory issuance as part of incident record, NIST IR-8 (Incident Response Plan) — update IR plan to codify fallback authority hierarchy when CISA advisory is absent, NIST AU-10 (Non-Repudiation) — maintain irrefutable records of intelligence source citations and compliance actions taken, NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Create a dated compliance memo (PDF with file hash recorded) documenting: (1) the KEV entry reference and deadline date, (2) the absence of a CISA standalone advisory as of the deadline, (3) citation of SANS ISC Diary update numbers (through Update 007, April 8, 2026) and Google GTIG UNC6780 reporting as the authoritative threat intelligence basis for remediation actions taken, (4) all remediation steps completed with timestamps and responsible parties. Store this in an immutable location (write-once S3 bucket, SharePoint with version history locked, or printed and signed). For regulated environments (FedRAMP, CMMC, PCI), include explicit mapping of which NIST 800-53 or CIS controls were addressed by each action to demonstrate control-level compliance independent of the CISA advisory.

Evidence: Archive the full text of each referenced SANS ISC Diary entry (SANS ISC Update 001 through Update 007) and Google GTIG UNC6780 reporting as PDFs with capture timestamps and SHA-256 hashes — these are your evidentiary basis for compliance decisions and may be unavailable or modified in the future. Preserve screenshots or exports of the CISA KEV catalog showing the entry and deadline alongside the absence of a linked CISA advisory at the deadline date, creating a contemporaneous record of the gap. Document the organizational decision log showing who reviewed the intelligence, what actions were authorized, and when — this establishes the chain of custody for compliance decisions made without a CISA advisory anchor.

Detection Guidance

Monitor for behavioral indicators: (1) Trivy process execution with unexpected command-line arguments, unusual parent processes, or execution outside scheduled scan windows; (2) Anomalous outbound network

connections from Trivy execution contexts; (3) Access to secret management systems, container registries, or source code repositories outside normal scanner scope; (4) Pipeline logs showing credential exfiltration or artifact staging to external repositories. Review CI/CD pipeline logs for failed authentication attempts followed by successful access using different credentials (lateral movement). Cross-reference SANS ISC Diary for updated IOCs as the campaign evolves.

Framework Mappings

MITRE-ATTACK

- **T1552.001** — Credentials In Files
- **T1610** — Deploy Container
- **T1554** — Compromise Host Software Binary
- **T1212** — Exploitation for Credential Access
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts
- **T1609** — Container Administration Command
- **T1195.002** — Compromise Software Supply Chain
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1213** — Data from Information Repositories

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **CM-3** — Configuration Change Control
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552.001	Credentials In Files	Credential-Access
T1610	Deploy Container	Defense-Evasion
T1554	Compromise Host Software Binary	Persistence
T1212	Exploitation for Credential Access	Credential-Access
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T1609	Container Administration Command	Execution
T1195.002	Compromise Software Supply Chain	Initial-Access

Technique ID	Technique Name	Tactic
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1213	Data from Information Repositories	Collection

Sources

Source	URL	Tier
Security News	https://www.sans.org/white-papers/when-security-scanner-became-weapon	T3
Cisco source code stolen in Trivy-linked dev environment breach	https://www.bleepingcomputer.com/news/security/cisco-source-code-st...	T3
Cisco Source Code Stolen in Trivy Supply Chain Attack - Safestate	https://www.safestate.com/post/cisco-source-code-stolen-in-trivy-su...	T3
Cisco source code stolen by ShinyHunters via Trivy supply-chain ...	https://www.reddit.com/r/netsec/comments/1sa8nld/cisco_source_code_...	T3
Cisco Breached: Source Code Stolen - Cybersecurity Today	https://www.youtube.com/watch?v=6tvc0uiGiH0	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-08 18:47 UTC by TJS Security Command Center