INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 16:27 UTC

Axios and Trivy Supply Chain Compromises Expose Hundreds of Thousands of Secrets; OpenAI Certificate Revocation Deadline Set for May 8

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0170
Type	Threat Campaign
CVE ID	CVE-2026-33634
Severity	HIGH
CVSS Base Score	9.5
EPSS Score	0.2115 (96th percentile)
Affected Products	Axios npm package (all versions distributed during compromise window), Trivy vulnerability scanner (Aqua Security), OpenAI ChatGPT Desktop / Codex / Codex CLI / Atlas (macOS), LiteLLM (PyPI), Telnyx Python SDK (PyPI), Checkmarx GitHub Actions workflows, European Commission Europa web hosting, Mercor
Published	2026-04-13T02:50:00
Discovery Source	Rss

Executive Summary

Two coordinated supply chain attacks - one assessed by [source] to be linked to UNC1069 (North Korea-linked), one to financially motivated group TeamPCP - injected credential-stealing backdoors into the Axios npm package and the Trivy vulnerability scanner, tools used by millions of development and security teams worldwide. Downstream victims include OpenAI, the European Commission, and AI startup Mercor; Google's Threat Intelligence Group assessed that hundreds of thousands of secrets may have been exfiltrated. Stolen credentials are actively fueling ransomware, SaaS exploitation, and extortion campaigns, and OpenAI has set a hard May 8, 2026 deadline after which older macOS app versions will be blocked due to a compromised signing certificate.

Technical Analysis

Two threat actors conducted separate but coordinated supply chain intrusions in March 2026. UNC1069 and TeamPCP (UNC6780, financially motivated) trojanized the Axios npm package and Aqua Security's Trivy

vulnerability scanner, embedding backdoors and credential-harvesting payloads into widely trusted developer tooling. CVE-2026-33634 (CVSS 9.5, EPSS 0.212 / 95.7th percentile) is assigned to the Trivy compromise (NOTE: the structured item data marks cisa_kev as false, but the technical narrative references KEV addition - cross-validate directly against https://www.cisa.gov/known-exploited-vulnerabilities-catalog before treating KEV status as confirmed). Root cause weaknesses: CWE-494 (Download of Code Without Integrity Check), CWE-829 (Inclusion of Functionality from Untrusted Control Sphere), CWE-295 (Improper Certificate Validation, relevant to the OpenAI certificate chain), and [verify whether CWE-798 applies or substitute with CWE-502 Deserialization or equivalent based on payload injection mechanism per Aqua Security advisory]. MITRE ATT&CK coverage spans T1195.001 and T1195.002 (Compromise Software Supply Chain, Development Tools and Software Dependencies), T1554 (Compromise Client Software Binary), T1072 (Software Deployment Tools), T1552.001 (Credentials in Files), T1041 (Exfiltration Over C2 Channel), T1071.001 (Web Protocols for C2), T1486 (Data Encrypted for Impact, ransomware follow-on), T1078/T1078.004 (Valid Accounts, cloud account abuse with stolen credentials), T1027 (Obfuscated Files or Information), T1570 (Lateral Tool Transfer), T1059 (Command and Scripting Interpreter). Secondary affected scope includes LiteLLM (PyPI), Telnyx Python SDK (PyPI), Checkmarx GitHub Actions workflows, European Commission Europa hosting, and Mercor. OpenAI's macOS app signing certificate was compromised within the attack chain; all macOS versions of ChatGPT Desktop, Codex, Codex CLI, and Atlas that predate the re-signed release will be revoked and blocked on May 8, 2026. Patch and remediation status should be validated against Aqua Security's GHSA-69fq-xp46-6x23 advisory and NVD entry for CVE-2026-33634 directly.

Action Checklist

1. Step 1: Containment. Immediately audit your dependency lists (package-lock.json, requirements.txt, Pipfile.lock) for Axios npm and Trivy versions installed during March 2026. Suspend any build systems or developer machines that executed these tools until they are patched. Rotate all secrets, API keys, tokens, and service account credentials that were accessible to these tools during the compromise window. For OpenAI macOS app users, identify all endpoints running ChatGPT Desktop, Codex, Codex CLI, or Atlas on macOS and confirm the installed version is current; versions predating the re-signed release will stop functioning after May 8, 2026.
2. Step 2: Detection. Query your SIEM and EDR for process execution of trivy or node processes spawning unexpected outbound connections (T1071.001, T1041). Search package manager logs and artifact registry pull logs for Axios versions matching the March 2026 compromise window. Inspect CI/CD pipeline logs (GitHub Actions, Jenkins, GitLab CI) for Checkmarx action invocations with anomalous parameters or unexpected network calls. Check cloud provider access logs (AWS CloudTrail, Azure Monitor, GCP Audit Logs) for API calls using credentials that were present in environments where compromised packages executed; focus on T1078.004 (cloud account abuse). Review endpoint telemetry for obfuscated script execution (T1027, T1059) originating from build or scan tooling. Refer to Aqua Security's GHSA-69fq-xp46-6x23 and CISA KEV supplemental data for specific IOC hashes, C2 domains, and IP addresses, which are maintained directly by the authoring vendors.
3. Step 3: Eradication. Pin Axios to a verified clean version confirmed by the npm registry integrity metadata and the package maintainer's post-incident advisory; do not re-introduce any version from the compromise window. Upgrade Trivy to the version designated clean in GHSA-69fq-xp46-6x23. Remove and re-provision any CI/CD runners or build agents that executed compromised tooling; do not attempt in-place remediation. For OpenAI macOS apps, uninstall affected versions and reinstall from the official download source after confirming the re-signed certificate is in place. Audit and remove any Checkmarx

GitHub Actions workflow versions that pulled compromised dependencies.

4. Step 4: Recovery. After rotating credentials, validate that no residual sessions remain active by auditing OAuth token grants, API key last-used timestamps, and active service account sessions across all affected SaaS platforms. Re-run your vulnerability scan baseline using a verified clean Trivy version to confirm scan integrity. Monitor for T1486 indicators (ransomware precursor activity) and SaaS anomaly alerts for 30 days post-remediation given confirmed ransomware follow-on activity. Confirm OpenAI macOS app functionality post-May 8 by validating installed version against the re-signed release.

5. Step 5: Post-Incident. This incident exposes three control gaps: (1) absence of software supply chain integrity verification - implement or enforce Sigstore/Cosign signing verification or equivalent for npm and container image pulls; (2) overly broad secret access in CI/CD pipelines - apply least-privilege scoping to all pipeline credentials and enforce short-lived tokens via OIDC federation; (3) insufficient monitoring of developer tooling network behavior - extend EDR and network monitoring coverage to build systems and security scanning infrastructure, which are frequently excluded from standard monitoring scope. Map remediation to NIST SP 800-161r1 (Cybersecurity Supply Chain Risk Management), NIST CSF Govern (GV-1, GV-2), Protect (PR-3, PR-6), and Detect (DE-2), and CISA's Secure Software Development guidance.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, legal counsel, and breach notification counsel if CloudTrail, Azure Monitor, or GCP Audit Logs confirm API calls using credentials known to have been in scope during the Axios or Trivy compromise window, particularly any `GetSecretValue`, `AssumeRole`, or data-plane read/write operations that could indicate PII, PHI, or regulated financial data access triggering GDPR Article 33, HIPAA §164.412, or state breach notification obligations; additionally escalate if any T1486 ransomware precursor indicators (VSS deletion, mass file encryption) are observed on rebuilt systems, consistent with TeamPCP's confirmed ransomware follow-on pattern.
Recovery Notes	After credential rotation and runner re-provisioning, validate completeness by re-running the full CI/CD pipeline against a canary repository with no production access and confirming zero unexpected outbound network connections from Axios or Trivy processes using `tcpdump` on the runner host. Monitor all cloud provider access logs and SaaS audit trails for 30 days for any use of the rotated (now invalid) credential values — any hit indicates a credential copy was missed and requires an additional rotation cycle. Given TeamPCP's confirmed ransomware follow-on behavior and UNC1069's nation-state affiliation, treat any anomalous file encryption activity or new persistence mechanisms discovered on CI infrastructure during this window as a potential active intrusion requiring full incident restart rather than a recovery artifact.

Forensic Artifacts	npm registry pull logs and package-lock.json integrity hashes: The compromised Axios package would have a SHA-512 integrity value in package-lock.json that does not match the legitimate package hash published by the axios maintainer post-incident — this mismatch is the primary artifact distinguishing a poisoned install from a clean one. | CI/CD runner network flow records (NetFlow, VPC Flow Logs, or tcpdump captures): UNC1069 and TeamPCP credential-stealing backdoors in Axios and Trivy would produce outbound POST or DNS exfiltration traffic from node or trivy processes to C2 infrastructure outside npm registry (registry.npmjs.org) and Docker Hub CIDR ranges during build and scan job execution. | AWS CloudTrail / Azure Monitor / GCP Audit Logs filtered on CI service account identity: Any GetSecretValue, AssumeRole, ListBuckets, or IAM modification events attributed to service account keys present in compromised pipeline environments are direct evidence of T1078.004 cloud account abuse by the threat actors following credential exfiltration from the backdoored Axios or Trivy packages. | Sysmon Event ID 1 (Process Creation) and Event ID 3 (Network Connection) on CI runner hosts: Malicious code injected into Axios (a JavaScript HTTP client) or Trivy (a Go binary) would spawn as child processes of node or trivy respectively and initiate network connections — the parent-child process relationship and destination IP constitute threat-specific behavioral artifacts distinguishing backdoor execution from legitimate tool operation. | macOS Unified Log and codesign verification output for OpenAI ChatGPT Desktop, Codex, Codex CLI, and Atlas: Pre-re-signed versions of these apps carry a revoked certificate; the macOS Gatekeeper quarantine log and `codesign -vvv` output will show the specific Team ID and certificate serial number, establishing which endpoint was running an untrusted binary and whether any anomalous subprocess execution or keychain access occurred before the May 8 revocation deadline.

Per-Action IR Details

Step 1: Containment — Immediately audit your dependency manifests (package-lock.json, requirements.txt, Pipfile.lock) and CI/CD pipeline configurations for Axios npm package versions installed during March 2026 and Trivy versions pulled during the same window. Isolate any build systems, developer workstations, or CI runners that executed compromised versions. Rotate all secrets — API keys, tokens, service account credentials — that were accessible to these tools during the compromise window. For OpenAI macOS app users, identify all endpoints running ChatGPT Desktop, Codex, Codex CLI, or Atlas on macOS and assess whether the installed version predates the re-signed release; these versions will stop functioning after May 8, 2026.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-4 (Information Flow Enforcement), NIST CM-3 (Configuration Change Control), NIST IA-5 (Authenticator Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Run `npm ls axios --all` and `cat package-lock.json | grep -A3 '"axios"'` in each repository to identify installed versions; cross-reference resolved hashes against npm registry integrity metadata for March 2026 packages. For Trivy, execute `trivy --version` on all CI runners and correlate against the clean version specified in GHSA-69fq-xp46-6x23. Use `osquery` with `SELECT name, version, install_time FROM npm_packages WHERE name='axios'` to sweep developer workstations. Revoke and reissue secrets via each platform's CLI (e.g., `aws iam delete-access-key`, `gh auth token revoke`) before re-issuing short-lived replacements.

Evidence: Before isolating CI runners, preserve: (1) the full `package-lock.json` and `yarn.lock` from every build workspace showing the resolved Axios version and its integrity hash as it existed during the compromise window; (2) CI/CD job logs (GitHub Actions `workflow_run` logs, Jenkins build console output, GitLab CI job traces) timestamped to March 2026 showing which Axios and Trivy versions were pulled and from which registry; (3) environment variable dumps or CI secrets vault audit logs showing which credentials (API keys, tokens) were in scope during compromised

pipeline runs; (4) macOS endpoint inventory showing ChatGPT Desktop, Codex, Codex CLI, or Atlas version strings — collect via `mdls -name kMDItemVersion /Applications/ChatGPT.app` or equivalent before uninstall.

Step 2: Detection — Query your SIEM and EDR for process execution of trivy or node processes spawning unexpected outbound connections (T1071.001, T1041). Search package manager logs and artifact registry pull logs for Axios versions matching the March 2026 compromise window. Inspect CI/CD pipeline logs (GitHub Actions, Jenkins, GitLab CI) for Checkmarx action invocations with anomalous parameters or unexpected network calls. Check cloud provider access logs (AWS CloudTrail, Azure Monitor, GCP Audit Logs) for API calls using credentials that were present in environments where compromised packages executed — focus on T1078.004 (cloud account abuse). Review endpoint telemetry for obfuscated script execution (T1027, T1059) originating from build or scan tooling. IOC specifics should be sourced from Aqua Security's GHSA-69fq-xp46-6x23 advisory and CISA's KEV entry once KEV status is confirmed.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, use Sysmon (Event ID 3 — Network Connection) filtered for `trivy.exe` or `node.exe` parent processes initiating outbound connections to non-registry destinations; deploy the Sigma rule `proc_creation_win_node_network_connection.yml` adapted for build-agent hosts. Query AWS CloudTrail locally with `aws cloudtrail lookup-events --lookup-attributes AttributeKey=Username,AttributeValue=` filtering for `CreateAccessKey`, `AssumeRole`, or `GetSecretValue` calls outside normal pipeline windows. For Axios-specific exfiltration detection, run Wireshark or `tcpdump -w capture.pcap -i any host ` during a controlled re-execution of the suspect build, then inspect for POST requests to non-npm, non-GitHub destinations. Use `jq` against CloudTrail JSON exports to pivot on any access key IDs known to have been in compromised pipeline environments.

Evidence: Capture before analysis: (1) Sysmon Event ID 3 (Network Connection) logs from CI runner hosts showing `node` or `trivy` processes initiating outbound TCP connections — UNC1069 credential-stealers typically beacon to C2 infrastructure distinct from npm/Docker registry endpoints; (2) AWS CloudTrail `GetSecretValue`, `ListBuckets`, `AssumeRole`, and `CreateLoginProfile` events attributed to service account keys that were exposed in Axios/Trivy build environments during March 2026 — these indicate T1078.004 cloud account abuse by TeamPCP or UNC1069 post-exfil; (3) npm audit log at `~/.npm/_logs/` and Artifactory/Nexus pull logs showing exact package checksums resolved for Axios during the compromise window; (4) Checkmarx GitHub Actions `workflow_run` webhook payloads and runner diagnostic logs showing action version pinning and any `curl` or `wget` subprocess calls spawned during scan jobs; (5) macOS Unified Log entries (`log show --predicate 'process == "ChatGPT"' --info`) on endpoints running pre-re-signed OpenAI apps for anomalous subprocess execution or network activity.

Step 3: Eradication — Pin Axios to a verified clean version confirmed by the npm registry integrity metadata and the package maintainer's post-incident advisory; do not re-introduce any version from the compromise window. Upgrade Trivy to the version designated clean in GHSA-69fq-xp46-6x23. Remove and re-provision any CI/CD runners or build agents that executed compromised tooling — do not attempt to clean in place. For OpenAI macOS apps, uninstall affected versions and reinstall from the official download source after confirming the re-signed certificate is in place. Audit and remove any Checkmarx GitHub Actions workflow versions that pulled compromised dependencies.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), NIST IR-4 (Incident Handling), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Verify Axios integrity before re-introduction with `npm pack axios@ && shasum -a 512 axios-.tgz` and compare against the `integrity` field in the post-incident npm registry metadata. For Trivy, validate the clean binary using `cosign verify-blob` with Aqua Security's published signing key if available via GHSA-69fq-xp46-6x23. Re-provision CI runners using immutable infrastructure — destroy and rebuild from a known-good Docker image or VM snapshot predating March 2026, then lock the base image digest in your Dockerfile (`FROM @sha256:`). Pin Checkmarx GitHub Actions to a specific commit SHA (`uses: checkmarx/action@`) rather than a mutable tag. On macOS, verify the re-signed OpenAI certificate using `codesign -vvv /Applications/ChatGPT.app` before relying on the reinstalled app.

Evidence: Preserve before re-provisioning runners: (1) full disk image or filesystem snapshot of each compromised CI runner (use `dd` or cloud provider snapshot API) — UNC1069-attributed backdoors may have installed persistence mechanisms (cron jobs, systemd units, or launchd plists on macOS) that must be documented before destruction; (2) npm cache directories (`~/.npm/`, `/root/.npm/`, or runner-local cache paths) containing the compromised Axios tarball with its original SHA-512 integrity hash as evidence of the specific malicious version artifact; (3) Trivy binary hash (`sha256sum $(which trivy)`) from compromised runners before decommission; (4) GitHub Actions runner diagnostic logs (`_diag/` directory on self-hosted runners) showing workflow execution context during Checkmarx action invocations; (5) macOS keychain state and certificate trust store from affected endpoints before uninstall, to document whether the pre-re-signed OpenAI app performed any anomalous certificate operations.

Step 4: Recovery — After rotating credentials, validate that no residual sessions remain active by auditing OAuth token grants, API key last-used timestamps, and active service account sessions across all affected SaaS platforms. Re-run your vulnerability scan baseline using a verified clean Trivy version to confirm scan integrity. Monitor for T1486 indicators (ransomware precursor activity) and SaaS anomaly alerts for 30 days post-remediation given confirmed ransomware follow-on by TeamPCP. Confirm OpenAI macOS app functionality post-May 8 by validating installed version against the re-signed release.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST AC-4 (Information Flow Enforcement), NIST SI-3 (Malicious Code Protection), NIST CP-10 (System Recovery and Reconstitution), CIS 6.2 (Establish an Access Revoking Process), CIS 5.3 (Disable Dormant Accounts)

Compensating: Audit residual OAuth sessions without a CASB by querying each SaaS platform's native token management: GitHub (`gh api /applications//tokens`), AWS (`aws iam list-access-keys --user-name ` plus `aws iam get-access-key-last-used`), and GCP (`gcloud iam service-accounts keys list`). For TeamPCP ransomware precursor monitoring, deploy a YARA rule scanning for known ransomware staging behaviors (volume shadow copy deletion via `vssadmin delete shadows`, `wbadmin delete catalog`) on rebuilt CI runners using `yara -r rule.yar /proc/` on Linux runners. Re-run Trivy baseline scans with `trivy image --format json --output baseline-$(date +%F).json ` and store output for integrity comparison. Monitor GitHub audit log (`gh api /orgs//audit-log --paginate`) for anomalous Actions workflow triggers or new secret access for 30 days.

Evidence: Before declaring recovery complete, collect and retain: (1) API key last-used timestamps and OAuth token grant lists from all SaaS platforms (GitHub, OpenAI API, AWS, GCP, Azure) where credentials were accessible during the compromise — these establish the boundary of potential exfiltration scope attributable to UNC1069 and TeamPCP; (2) Trivy scan output JSON from the first clean baseline run, signed with a team GPG key to establish post-incident integrity baseline; (3) cloud provider access logs for the 30-day monitoring window showing any use of previously rotated credentials (indicates incomplete rotation or credential reuse); (4) endpoint detection telemetry from rebuilt CI runners for T1486-related activity — specifically VSS deletion commands, ransom note file creation patterns, or anomalous encryption of build artifact directories consistent with TeamPCP ransomware follow-on TTPs.

Step 5: Post-Incident — This incident exposes three control gaps: (1) absence of software supply chain integrity verification — implement or enforce Sigstore/Cosign signing verification or equivalent for npm and container image pulls; (2) overly broad secret access in CI/CD pipelines — apply least-privilege scoping to all pipeline credentials and enforce short-lived tokens via OIDC federation; (3) insufficient monitoring of developer tooling network behavior — extend EDR and network monitoring coverage to build systems and

security scanning infrastructure, which are frequently excluded from standard monitoring scope. Map remediation to NIST SP 800-161r1 (Cybersecurity Supply Chain Risk Management) and CISA's Secure Software Development guidance.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SA-12 (Supply Chain Protection), NIST AC-6 (Least Privilege), NIST AU-2 (Event Logging), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Implement Sigstore/Cosign verification in CI pipelines at no cost: add `cosign verify @` as a mandatory pipeline step before any `docker pull` or `trivy image` invocation, using Sigstore's public Rekor transparency log for npm package provenance where supported. Enforce OIDC-based short-lived tokens in GitHub Actions by replacing static `AWS_ACCESS_KEY_ID` secrets with the `aws-actions/configure-aws-credentials` action using `role-to-assume` — this eliminates long-lived keys accessible to a compromised Axios or Trivy dependency. Deploy Sysmon on all CI runner hosts with a configuration capturing Event ID 3 (network connections) and Event ID 1 (process creation) for `node`, `trivy`, and `python` processes, and forward to a centralized syslog receiver (e.g., Graylog CE) to close the monitoring gap on build infrastructure that UNC1069 and TeamPCP exploited by targeting tooling outside standard EDR scope.

Evidence: For the lessons-learned record, compile: (1) timeline reconstruction of when compromised Axios and Trivy versions first entered the environment versus when detection occurred — this gap directly measures the effectiveness of current supply chain monitoring controls and should drive SLA targets for future SBOM-based alerting; (2) complete inventory of secrets confirmed in-scope during the compromise window, categorized by sensitivity tier (production API keys vs. dev tokens vs. service accounts), to support regulatory breach notification assessment if PII or PHI was accessible; (3) network flow records showing any Axios or Trivy process communications to non-registry external IPs during the compromise window — these constitute the strongest forensic evidence of data exfiltration attributable to UNC1069 or TeamPCP and are required if law enforcement referral is pursued; (4) documentation of any Checkmarx GitHub Actions workflow runs that invoked compromised dependencies, preserving the exact action SHA and workflow YAML as evidence of the third-party action supply chain vector.

Detection Guidance

Primary detection targets: (1) Network - alert on outbound connections from trivy processes or node/npm processes to non-expected destinations, particularly during CI/CD pipeline execution windows; correlate with T1041 and T1071.001. (2) Endpoint/EDR - hunt for child processes spawned by trivy, npm install, or npx executions that invoke shell interpreters (bash, sh, cmd, powershell) or make direct socket connections; this maps to T1059 and T1554. (3) Secrets exposure - search source code repositories, environment variable stores, and artifact logs for credentials that were present in environments where Axios or Trivy executed during March 2026; prioritize API keys for OpenAI, cloud providers, and SaaS platforms given the confirmed downstream victim profile. (4) Cloud access logs - query for API activity from service accounts or tokens accessible to affected build environments, focusing on privilege escalation attempts, unusual resource creation, and cross-account access (T1078, T1078.004). (5) Package integrity - compare installed Axios package hashes against the npm registry integrity field for the same version; tampering will produce a mismatch. Refer to Aqua Security's GHSA-69fq-xp46-6x23 and CISA KEV supplemental data for specific IOC hashes, C2 domains, and IP addresses, which are maintained directly by the authoring vendors.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23`	Aqua Security official security advisory for Trivy supply chain compromise — primary source for IOC hashes, affected versions, and C2 indicators	HIGH
URL	`https://nvd.nist.gov/vuln/detail/CVE-2026-33634`	NVD entry for CVE-2026-33634 (CVSS 9.5) — cross-validate affected version ranges and supplemental IOC data here	HIGH

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1059** — Command and Scripting Interpreter
- **T1588.002** — Tool
- **T1072** — Software Deployment Tools
- **T1071.001** — Web Protocols
- **T1552.001** — Credentials In Files
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1195.002** — Compromise Software Supply Chain
- **T1486** — Data Encrypted for Impact
- **T1078.004** — Cloud Accounts
- **T1027** — Obfuscated Files or Information
- **T1554** — Compromise Host Software Binary
- **T1570** — Lateral Tool Transfer
- **T1588.004** — Digital Certificates

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services

- **SR-3** — Supply Chain Controls and Processes
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-3** — Configuration Change Control
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures
- **A02:2021** — Cryptographic Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059	Command and Scripting Interpreter	Execution
T1588.002	Tool	Resource-Development
T1072	Software Deployment Tools	Execution
T1071.001	Web Protocols	Command-And-Control
T1552.001	Credentials In Files	Credential-Access
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1078.004	Cloud Accounts	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1554	Compromise Host Software Binary	Persistence
T1570	Lateral Tool Transfer	Lateral-Movement
T1588.004	Digital Certificates	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/openai-revokes-macos-app-certific...	T3
CVE-2026-33634 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33634	T1
CVE-2026-33634 Aquasecurity Trivy Embedded Malicious ... - Rapid7	https://www.rapid7.com/db/vulnerabilities/trivy-cve-2026-33634/	T3
CISA sounds alarm on Langflow RCE, Trivy supply chain ...	https://www.helpnetsecurity.com/2026/03/27/cve-2026-33017-cve-2026-...	T3

Source	URL	Tier
Trivy ecosystem supply chain temporarily compromised - GitHub	https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq...	T3

Generated 2026-04-13 16:27 UTC by TJS Security Command Center