INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-03 13:37 UTC

TeamPCP Exploits Trivy Supply-Chain Flaw to Breach European Commission AWS Accounts, Exposing 71 EU Entities

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0141
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Amazon Web Services (AWS) - European Commission accounts; Trivy (supply-chain vector); LiteLLM PyPI package; Europa.eu web hosting; GitHub; PyPI; NPM; Docker
Published	2026-04-03T02:33:34
Discovery Source	Rss

Executive Summary

On March 10, 2026, threat group TeamPCP breached the European Commission's AWS environment using an API key stolen during a supply-chain attack on the Trivy security scanner. The intrusion exposed data from EU government entities; ShinyHunters subsequently published a dataset on a dark web leak site. CERT-EU confirmed attribution on April 3, 2026. The primary business risk is unauthorized access to sensitive government data through compromised cloud credentials and third-party dependency integrity failures. [Note: Initial reporting cited 30 entities; later reports referenced up to 71. Verify official CERT-EU count for accurate scope.]

Technical Analysis

TeamPCP gained initial access via a compromised API key traced to the Trivy supply-chain attack (T1195.002). The LiteLLM PyPI package was identified as a malicious component in the broader campaign, documented by Datadog Security Labs. Attackers used TruffleHog to scan for exposed secrets in the EC's AWS environment (T1552.001, T1552.004), then created covert IAM access keys to establish persistence (T1078.004, T1098, T1528). Data from EU government entities was exfiltrated via cloud storage (T1530, T1537) and published externally (T1567.002). Relevant weaknesses: CWE-284 (improper access control), CWE-522 (insufficiently protected credentials), CWE-200 (exposure of sensitive information), CWE-732 (incorrect permission assignment), CWE-494 (download of code without integrity check). No NVD CVE is assigned to this campaign. MITRE coverage includes T1087.004 (cloud account enumeration) and T1588.001 (tool acquisition). Affected

platforms: AWS (EC accounts), Trivy (supply-chain vector), LiteLLM PyPI package, GitHub, PyPI, NPM, Docker, Europa.eu hosting.

Action Checklist

1. Step 1: Containment. Immediately audit all AWS IAM users and roles across your organization for unrecognized or recently created access keys. Revoke any keys that cannot be traced to authorized provisioning. If Trivy, LiteLLM, or related tooling is deployed in CI/CD pipelines with cloud credentials, rotate those credentials now and scope IAM permissions to least privilege. Reference: AWS IAM credential report and CloudTrail CreateAccessKey events.
2. Step 2: Detection. Query CloudTrail for CreateAccessKey, ListAccessKeys, and AssumeRole events from unexpected principals or unusual source IPs, especially within CI/CD runner IP ranges. Search pipeline logs and dependency manifests for compromised LiteLLM PyPI package versions identified in the Datadog Security Labs report (https://securitylabs.datadoghq.com/articles/litellm-compromised-pypi-teampcp-supply-chain-campaign/; consult advisory for affected version range). Run TruffleHog (https://github.com/trufflesecurity/trufflehog) or equivalent secret scanning against all repositories that have cloud credential access. Look for outbound data transfers to non-standard S3 buckets or external endpoints (CloudTrail S3 and data events, VPC Flow Logs).
3. Step 3: Eradication. Remove or pin the compromised LiteLLM PyPI package versions per Datadog's advisory (https://securitylabs.datadoghq.com/articles/litellm-compromised-pypi-teampcp-supply-chain-campaign/). Verify integrity of all Trivy installations against official release hashes from the Aqua Security GitHub repository. Enforce dependency pinning with hash verification (pip --require-hashes, npm lockfiles with integrity checks) across all pipelines. Remove any IAM access keys not provisioned through your approved identity lifecycle process.
4. Step 4: Recovery. Re-validate all cloud credentials in use by CI/CD systems, security tooling, and automation after rotation. Enable AWS GuardDuty and review findings for credential exfiltration indicators (UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration, Policy:IAMUser/RootCredentialUsage). Monitor CloudTrail for 30 days post-remediation for recurrence of CreateAccessKey or cross-account role assumption from pipeline contexts. Confirm no persistent Lambda functions, EC2 instance profiles, or scheduled tasks were created under compromised principals.
5. Step 5: Post-Incident. This attack exposed three systemic control gaps: absence of secrets scanning in CI/CD pipelines before credential use, no integrity verification on third-party security tooling (Trivy) and PyPI dependencies (LiteLLM), and over-permissioned IAM roles attached to build systems. Remediation priorities: implement OIDC-based short-lived credentials for CI/CD instead of static API keys (eliminates the stolen key attack surface), enforce software supply-chain controls per NIST SP 800-218 (SSDF) and SLSA framework, and introduce mandatory dependency integrity checks (hash pinning, SBOM generation) as pipeline gates.

Detection Guidance

Note: Public IOC data (file hashes, C2 IPs, exfil endpoints) is not available from source data. Detection relies on behavioral indicators (CloudTrail events, dependency scanning, dark web monitoring) rather than

signature-based matching. Primary detection surface is AWS CloudTrail. Query for: (1) CreateAccessKey events where the requesting principal is a service account, IAM role, or unknown user, especially if the source IP resolves to a CI/CD runner, PyPI package execution context, or unfamiliar ASN. (2) ListBuckets, GetObject, or PutObject events at unusual volumes or times from programmatic principals. (3) AssumeRole events across account boundaries not matching your approved cross-account role inventory. Secondary detection: audit your Python dependency tree for the specific compromised LiteLLM versions identified in the Datadog Security Labs report (see https://securitylabs.datadoghq.com/articles/litellm-compromised-pypi-teampcp-supply-chain-campaign/ for affected version matrix), compare installed versions against the advisory. Run TruffleHog (https://github.com/trufflesecurity/trufflehog) against all repositories with cloud access. Behavioral indicator: TruffleHog was used by the attackers internally; detecting its execution within your environment from an unexpected context may indicate active credential harvesting. Monitor dark web leak sites and paste sites for your organization's domain strings as a post-breach indicator.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://securitylabs.datadoghq.com/articles/litellm-compromised-pypi-teampcp-supply-chain-campaign/`	Datadog Security Labs report on LiteLLM PyPI compromise and TeamPCP supply-chain campaign — reference for affected package versions	MEDIUM
DOMAIN	`pypi.org`	Distribution channel for compromised LiteLLM package used by TeamPCP; monitor outbound connections from build systems to PyPI for unexpected package pulls	LOW

Framework Mappings

MITRE-ATTACK

- **T1552.004** — Private Keys
- **T1078.004** — Cloud Accounts
- **T1098** — Account Manipulation
- **T1528** — Steal Application Access Token
- **T1552.001** — Credentials In Files
- **T1567.002** — Exfiltration to Cloud Storage
- **T1537** — Transfer Data to Cloud Account
- **T1588.001** — Malware
- **T1087.004** — Cloud Account
- **T1195.002** — Compromise Software Supply Chain
- **T1530** — Data from Cloud Storage

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
- **AC-3** — Access Enforcement
- **IA-5** — Authenticator Management
- **SC-28** — Protection of Information at Rest
- **AC-6** — Least Privilege
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.2** — Use Unique Passwords
- **3.3** — Configure Data Access Control Lists
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552.004	Private Keys	Credential-Access

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1098	Account Manipulation	Persistence
T1528	Steal Application Access Token	Credential-Access
T1552.001	Credentials In Files	Credential-Access
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1537	Transfer Data to Cloud Account	Exfiltration
T1588.001	Malware	Resource-Development
T1087.004	Cloud Account	Discovery
T1195.002	Compromise Software Supply Chain	Initial-Access
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/cert-eu-european-com...	T3
	https://www.bleepingcomputer.com/news/security/cert-eu-european-com...	T3
	https://www.bleepingcomputer.com/news/security/european-commission-...	T3
	https://www.bleepingcomputer.com/news/security/panera-bread-data-br...	T3
LiteLLM and Telnyx compromised on PyPI - Datadog Security Labs	https://securitylabs.datadoghq.com/articles/litellm-compromised-pyp...	T3

Generated 2026-04-03 13:37 UTC by TJS Security Command Center