certego

SEGNALI DEBOLI

Tecniche emergenti e
pattern di attacco osservati
dal SecOps di Certego

LiteLLM compromesso: supply chain attack via PyPI

Read more →

certego

Cosa sta succedendo?

Negli ultimi giorni, il nostro SecOps Team ha rilevato diverse istanze applicative che eseguono una versione malevola di **LiteLLM**.

Le release coinvolte sono:

✕ 1.82.7 e 1.82.8

Le versioni sicure sono:

✓ ≤ 1.82.6

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Attacco a LiteLLM

Tipologia:

Software supply chain attack.

Obiettivo:

Compromettere ambienti di sviluppo, pipeline CI/CD e infrastrutture cloud attraverso una dipendenza legittima.

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Threat Actor: TeamPCP

Noto anche come PCPcat, Persy_PCP, ShellForce e DeadCatx3, è lo stesso gruppo associato alla compromissione di **Trivy**, poi sfruttata come vettore nella catena d’attacco verso LiteLLM.

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Perché è critico?

Non si presenta come malware tradizionale.

Si nasconde in un pacchetto ritenuto affidabile e si attiva in più fasi, consentendo di:

- Sottrarre credenziali cloud
- Raccogliere chiavi SSH
- Esfiltrare token Kubernetes
- Installare una backdoor persistente
- Favorire movimenti laterali in ambienti containerizzati

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Dinamica dell’attacco

La catena d’attacco si sviluppa lungo la supply chain:

- Compromissione delle credenziali del publisher PyPI
- Abuso della Trivy GitHub Action nella pipeline CI/CD di LiteLLM
- Pubblicazione di versioni malevole su PyPI
- Esecuzione del payload sugli host che installano il pacchetto

Dominio di esfiltrazione osservato:

```
models[.]litellm[.]cloud
```

certego

MITRE ATT&CK

T1546.018
Python Startup Hooks

T1003
Credential Dumping

T1610
Deploy Container

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Remediation

Si consiglia di:

- Verificare la presenza di LiteLLM 1.82.7 / 1.82.8
- Eseguire il rollback a ≤ 1.82.6
- Considerare compromessi i secret presenti sugli host impattati
- Ruotare credenziali cloud, chiavi SSH e token Kubernetes
- Verificare eventuali meccanismi di persistenza, rivedere pipeline CI/CD, package mirror e dipendenze non version-pinned

SecOps Services
SECURITY OPERATIONS SERVICES

certego

PURE-PLAY

MDR