CubeAPM Unauthenticated Log Injection Vulnerability

Reported by: Prasann Nuwal
Contact: +91 6377039073

An unauthenticated endpoint in CubeAPM allows anyone to inject arbitrary log data into the system. The vulnerable endpoint:

POST /api/logs/insert/elasticsearch/_bulk

accepts unauthenticated input, which leads to unauthorized log injection into production dashboards.

Proof of Concept:
curl -X POST "http://:3130/api/logs/insert/elasticsearch/_bulk" \ -H "Content-Type: application/x-ndjson" \ --data-binary $'{ "index": { "_index": "logs" } }\n { "@timestamp": "2025-08-07T09:20:00Z", "level": "critical", "message": "Before request [GET /kuchbhi, client=10.6.66.66]", "application": "bla", "service.name": "bla", "env": "dev", "subsystemName": "aws-waf-dev" }'

Security Impact: False Log Injection: Attackers can forge arbitrary log entries. **Log Poisoning:** Can distort alerting, dashboards, or performance metrics. **Attack Obfuscation:** High-volume injection can conceal real intrusions. **Denial of Service:** Abuse could impact pipeline performance and availability.

Scope:
This issue appears to stem from the CubeAPM package itself, not a deployment misconfiguration. Any deployment exposing this endpoint without upstream protection is vulnerable.

Affected Versions:
Confirmed on: 8.17.1, nightly-2025-08-01-1
Older versions are likely affected unless /api/logs/insert/elasticsearch/_bulk was protected earlier.

CVE Assignment:
As the original discoverer of this vulnerability, I intend to request a CVE via MITRE.
If the maintainers prefer to handle CVE assignment internally or via a CNA, I am happy to coordinate and be credited accordingly.
Otherwise, I will proceed to request a CVE within the standard 14-day coordinated disclosure window.

Thank you.
— Prasann Nuwal