ONAP pentest summary

Samsung R&D Institute Poland (Open Source Group)

13.06.2019

Report

https://wiki.onap.org/display/DW/ONAP+Casablanca+Security+Assessment

Assumptions

Environment	Casablanca deployed using OOM on K8s managed by Rancher
Nodes	non-compromised, vulnerability-free system software
K8s API	well-protected, no compromised nor external pods
Access	all ports exposed outside of cluster (NodePorts)

Result: Quite an exposure

Externally accessible ports	~100
Insecure communication (HTTP) also enabled	~60
Unprotected services (no authorization)	>10

Result: User management

- Anonymous user creation (via **unprotected** API endpoint)
- Encrypted password storage (instead of hashed; accessible via API endpoint)
- User impersonation: name declaration without asking for password

Result: Ease of use vs. security imbalance

- Arbitrary code execution via debugging tools (JDWP)
- Hardcoded passwords in OOM Helm charts

Recommendation: Removals

- Limit exposure, use HTTPS, migrate NodePorts to Ingress controller
- Use global user management service
  - Choose ONAP-wide uniform solution (AAF? Istio?)
  - Remove component-specific implementations

Recommendation: Adjustment

- Use safe (production grade-like) defaults:
  - separate *development* and *release* Docker container images
  - replace hardcoded passwords from OOM Helm charts
- Extend security tests (*Don't repeat errors of the past*)

Ongoing efforts: Present state

- Tracking information:
  - OSJI (Jira)
  - OSA (RTD, separate repository)
  - Security Release Notes (per project)

Ongoing efforts: Improvements

- ONAP Vulnerability Management
- Hardcoded OOM passwords removal
- Ingress controller migration investigation

Thank you

- That’s all