ONAP Security Best Practices

Krzysztof Opasiak

Samsung R&D Institute Poland

SAMSUNG

Agenda

- Introduction
- Network-related
- Code-related
- Deployment-related
- Others
- Summary
- Q & A

Introduction

SAMSUNG

Introduction

- **ONAP should be secure!**
- **Breach into internal network**
- **Malicious insider**
- **Maybe some regulations?**

Network-related

SAMSUNG

Only encrypted communication should be used

- **All ports exposed outside of cluster should use TLS**
- **Recommended version of TLS is 1.2**
- **Component-to-component communication should follow the same requirements**
- **Exceptions should be well justified and documented**

Number of exposed ports should be minimized

- **Every exposed service increase attack surface**
- **This increases the risk of security breach**
- **ONAP should expose only neccessary minimum of services outside of cluster**
- **We should not expose:**
  - Databases
  - Debug interfaces
- **Exceptions should be well justified and documented**

All APIs should be well protected

- **SSO and RBAC should be implemented**
- **Central credential management service**
- **All APIs should be protected**

Debuging tools should not be a part of release image

- **Release image/code should be treated as production**
- **Default configuration should be secure**
- **There should be no debugging tools on release image**
- **Yes, even if they are exposed only internally**
- **You can use override and multi-stage build if you need theme**

API doc should not be part of release image

- **Swagger is a very nice tool and we should use it**
- **API doc should be available somewhere on the net (readthedocs?)**
- **It should not be shipped on release images**

Code-related

SAMSUNG

SQL statement should be prepared before usage

- **BAD**

```
String query = "SELECT␣*␣FROM␣users␣WHERE␣userid␣='"
       + userid + "'" + "␣AND␣password='" + password + "'";
Statement stmt = connection.createStatement();
ResultSet rs = stmt.executeQuery(query);
```

- **GOOD**

```
PreparedStatement stmt = connection.prepareStatement(
       "SELECT␣*␣FROM␣users␣WHERE␣userid=?␣AND␣password=?");
stmt.setString(1, userid);
stmt.setString(2, password);
ResultSet rs = stmt.executeQuery();
```

Escape, Validate and Sanitize user input

- **All special characters in user input should be escaed**
- **User input should be validated (whitelist characters)**
- **Sanitize user input (prevent it from being executed)**

Don't propagate any crypto-related errors

- **Cryptography is sensitive...**
- **Knowledge about particular error may help attacker to break the crypto**
- **Cryptography-related errors should not be distingushable for user**

Deployment-related

SAMSUNG

Don't run as a root

- There is no such thing as a secure code
- There is always non 0 chance that someone will break some API
- We should reduce the consequences of such security brach
- That's why there should be no processes running as a root
- Unless it's absolutely neccessary but even then should be well documented

Harden your container

- **Disable stack traces by default**
- **Remove examples**
- **Change landing page**

Passwords, passwords, passwords evrywhere...

- **Probably no one really knows how many passwords we have in our charts**
- **Dozens of users is created during deployment**
- **All this stuff should be well documented and easy configurable**

Others

SAMSUNG

Make good security release notes

- **Typical security release note:**
- **Is it helpful?**
- **A good security release note should mention:**
  - All fixed security issues (esp. CVEs)
  - Identified security risks

Have some guidelines...

- **There is no such thing as global ONAP security guidelines**
- **Even worse there is no documentation for many ONAP services**
- **Not to mention service-specific security doc**
- **We should develop these...**

Summary

SAMSUNG

Summary

- **Security is not only CII badging**
- **It should be every day habit to create a secure code**
- **There is a long way ahead...**
- **But we need to start this journey now!**

Q & A

SAMSUNG

Thank you!

Krzysztof Opasiak

Samsung R&D Institute Poland

+48 605 125 174
k.opasiak@samsung.com