TILF NETWORKING

LFN Developer & Testing Forum

ONAP Honolulu CII Badging

Tony Hansen

2021-02-03



Honolulu Global Requirement



- CII Website Documentation reviews:
 - Crypto Credentials Agility
 - Implement Secure Design
- One Work Item for many projects:
 - Review any Crypto Weaknesses

https://jira.onap.org/browse/REQ-443

CII Website Document Reviews



For both reviews:

- Log into the CII website and check your answer
- 2. If your application can say "Yes, we do that", then click "Met"
- If your application is "Yes, we should do that but don't currently," then click "Not Met" and file a Jira ticket
- 4. If your application doesn't do this and doesn't need to do it, then click "Not Applicable"



Crypto Credentials Agility

Crypto Credentials Agility



- This CII Badging requirement says:
 - "The project MUST support storing authentication credentials (such as passwords and dynamic tokens) and private cryptographic keys in files that are separate from other information (such as configuration files, databases, and logs), and permit users to update and replace them without code recompilation.
 - If the project never processes authentication credentials and private cryptographic keys, select 'not applicable' (N/A)."

Notes:



 If all of your credentials come from OOM and are accessed through Kubernetes secrets (such as environment variables or mounted volumes), then you can safely answer "Met"



Implement Secure Design

Implement Secure Design



- This CII Badging requirement says:
 - "The project MUST implement secure design principles (from 'know_secure_design'), where applicable.
 - If the project is not producing software, select 'not applicable' (N/A).
- The CII details for this requirement say:
 - For example, the project results should have fail-safe defaults (access decisions should deny by default, and projects' installation should be secure by default).
 - They should also have complete mediation (every access that might be limited must be checked for authority and be non-bypassable).
 - Note that in some cases principles will conflict, in which case a choice must be made (e.g., many mechanisms can make things more complex, contravening 'economy of mechanism' / keep it simple).

Notes:



- This is a follow-on question from the Passing level badge question that at least one person on your team needs to "understand secure design".
- This question asks if you are actually doing it.

More Examples of Secure Design



"The Protection of Information in Computer Systems" Saltzer and Schroeder

- economy of mechanism
- fail-safe defaults
- complete mediation
- open design
- separation of privilege

- least privilege
- least common mechanism
- psychological acceptability
- limited attack surface
- input validation with allowlists, not denylists.



Review Crypto Weaknesses

Review Crypto Weaknesses



We will be writing Jira tickets on these

```
aai aai-common 9
    cacher 1
    model-loader 1
    rest-client 1
appc 20
ccsdk apps 2
    sli-adaptors 3
    sli-northbound 2
    sli-plugins 6
```

```
clamp 2
                      sdc 3
                      sdnc-northbound 1
dcaegen2
                      so 9
    collectors-
restconf 9
                      vfc-nfvo-driver
music 5
                          svnfm-huawei 2
optf cmso 12
                          vnfm-svnfm-nokiav2 3
    fgps 2
                      vid 2
    has 2
                      vnfsdk-ves-agent 1
portal 2
```

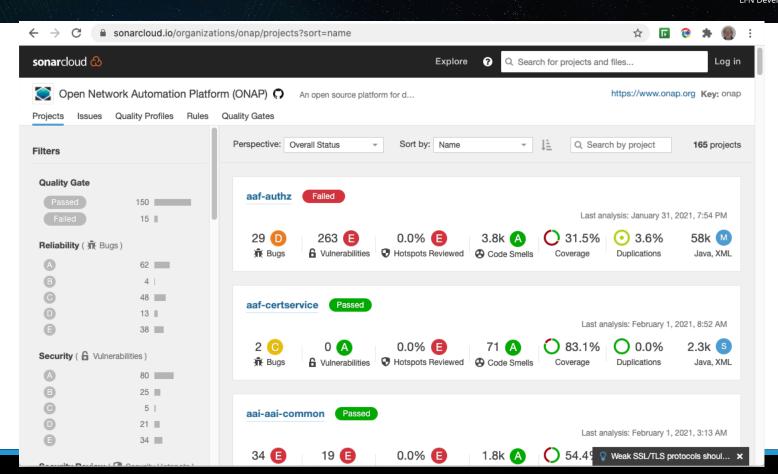
To Find All of The Issues



- Go to https://sonarcloud.io/organizations/onap/projects
- Click "Issues" (upper left)
- Click "Security Category" (center left)
- Click "Weak Cryptography"

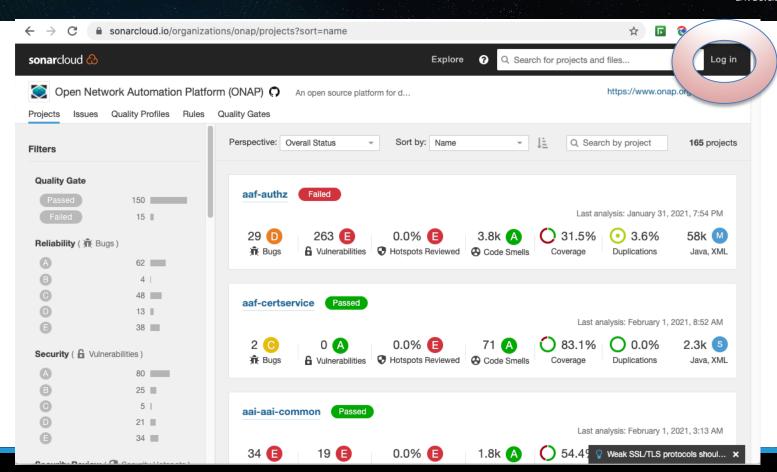
Go to https://sonarcloud.io/organizations/onap/projects





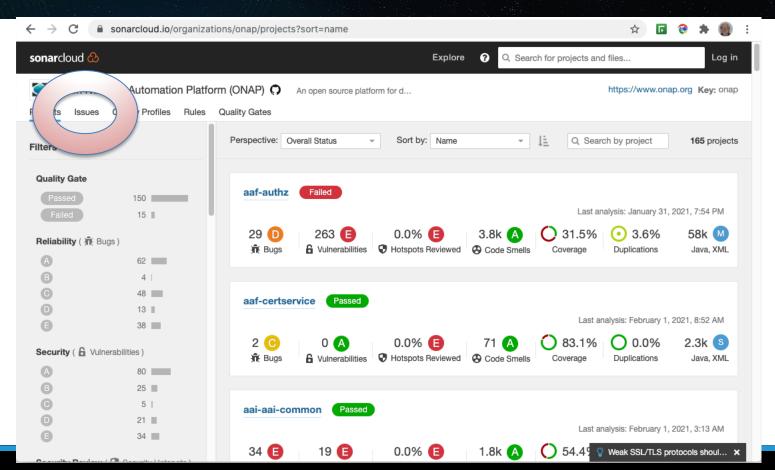
You Do Not Need to Login



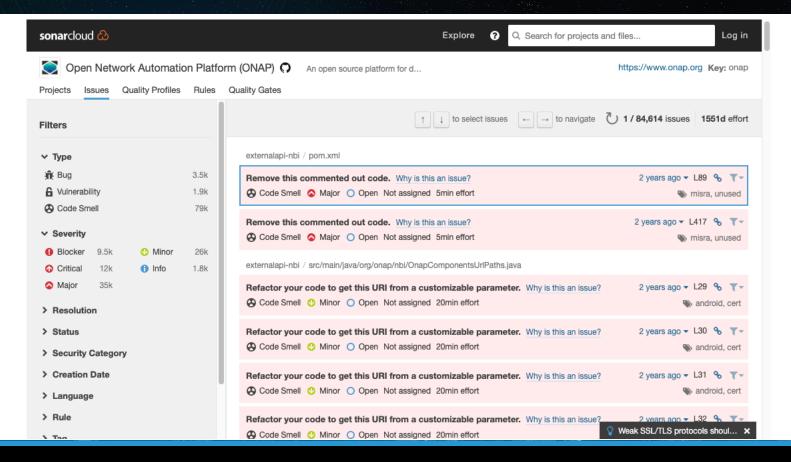


Click on "Issues"







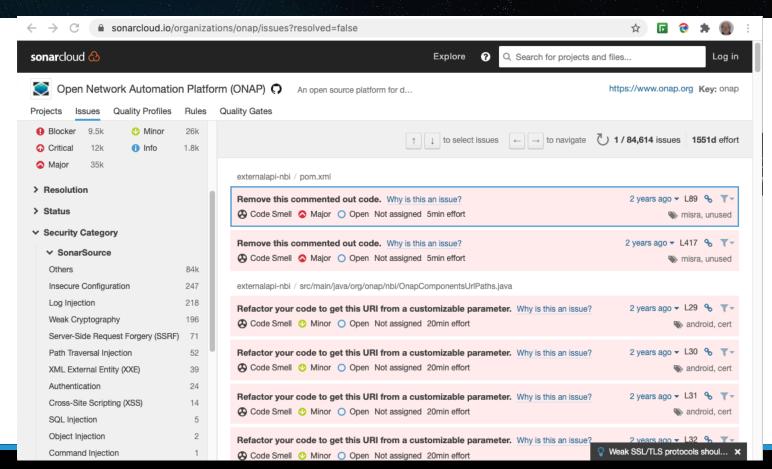


Click on "Security Category"



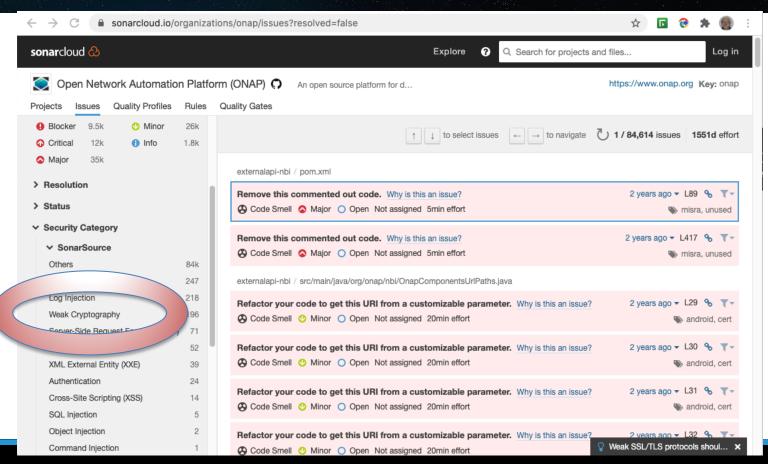
sonarcloud 🔕	Explore ? Q Search for projects	and files Log in
Open Network Automation Platfo	rm (ONAP) • An open source platform for d	https://www.onap.org Key: onap
Projects Issues Quality Profiles Rules	Quality Gates	
Filters	\uparrow \downarrow to select issues \longleftarrow \rightarrow to navigate	7 1 / 84,614 issues 1551d effort
➤ Type	externalapi-nbi / pom.xml	
∰ Bug 3.5k G Vulnerability 1.9k	Remove this commented out code. Why is this an issue? Code Smell Major Open Not assigned 5min effort	2 years ago ▼ L89 % ▼▼ misra, unused
Code Smell 79k Severity	Remove this commented out code. Why is this an issue? Code Smell Major Open Not assigned 5min effort	2 years ago ▼ L417 % ▼▼
● Blocker 9.5k	externalapi-nbi / src/main/java/org/onap/nbi/OnapComponentsUrlPaths.java	misra, unused
	Refactor your code to get this URI from a customizable parameter. Why is this an issue? © Code Smell Open Not assigned 20min effort	2 years ago ▼ L29 % ▼▼ Solution and and and and and and and and and an
> Security Category	Refactor your code to get this URI from a customizable parameter. Why is this an issue? © Code Smell Open Not assigned 20min effort	2 years ago ▼ L30 % ▼▼ water ago ▼ L30 % ▼▼
> Language	Refactor your code to get this URI from a customizable parameter. Why is this an issue? © Code Smell © Minor Open Not assigned 20min effort	2 years ago ▼ L31 % ▼▼ • android, cert
> Rule	Refactor your code to get this URI from a customizable parameter. Why is this an issue? Code Smell Minor Open Not assigned 20min effort	2 years ago ▼ L32 9 ▼ ▼ © Weak SSL/TLS protocols shoul ×



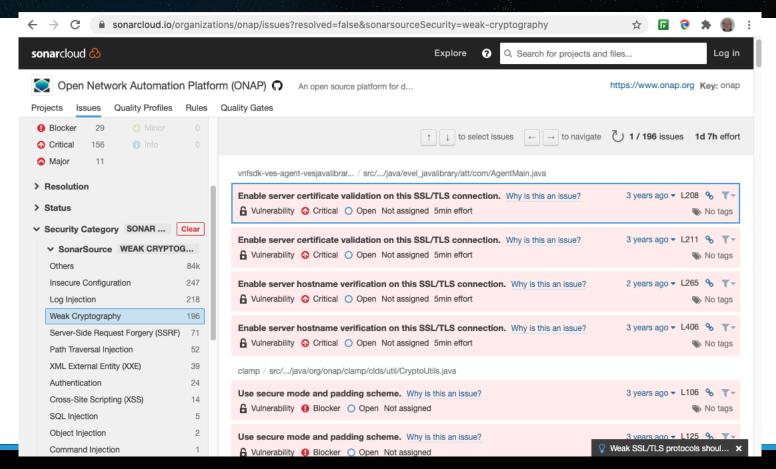


Click on "Weak Cryptography"









Drilling Down



Enable server certificate validation on this SSL/TLS connection. Why is this an issue?

3 years ago ▼ L208







clamp / src/.../java/org/onap/clamp/clds/util/CryptoUtils.java

Use secure mode and padding scheme. Why is this an issue?







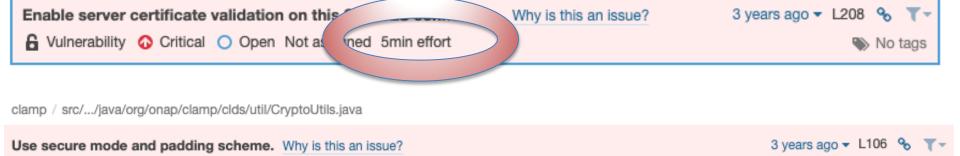




Note the Estimated Effort to Fix



No tags



Most common estimates: 2, 5 and 15 minutes. Not all have an estimate.

Note How Long Ago It Was Found



Enable server certificate validation on this SSL/TLS connection. Why is this an issue?





clamp / src/.../java/org/onap/clamp/clds/util/CryptoUtils.java

Use secure mode and padding scheme. Why is this an issue?





Vulnerability Blocker Open Not assigned



Direct Link to the Code



Enable server certificate validation on this SSL/TLS connection. Why is this an issue?







clamp / src/.../java/org/onap/clamp/clds/util/CryptoUtils.java

Use secure mode and padding scheme. Why is this an issue?

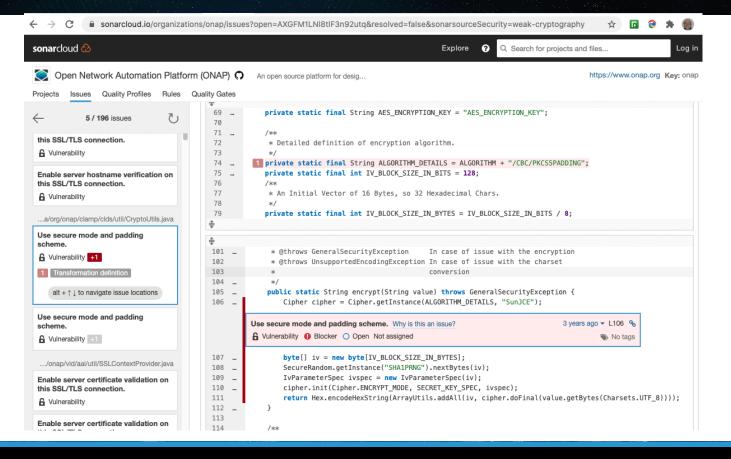






A View With the Code

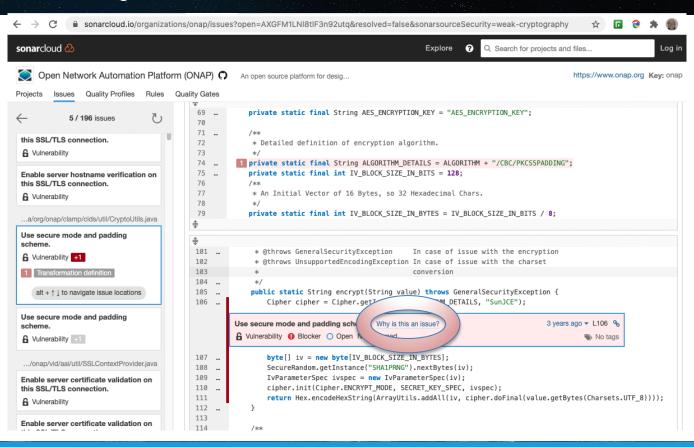




Each Jira ticket will go directly to this view

Click "Why is this an issue?"





Details on the issue



Encryption algorithms should be used with secure mode and padding scheme

Encryption algorithms should be used with secure mode and padding scheme

iava:S5542 9

Available Since Feb 17, 2020 SonarQube (Java)

To perform secure cryptography, operation modes and padding scheme are essentials and should be used correctly according to the encryption algorithm:

- For block cipher encryption algorithms (like AES), the GCM (Galois Counter Mode) mode that works internally with zero/no padding scheme, is recommended. At the opposite, these modes and/or schemes are highly discouraged:
 - . Electronic Codebook (ECB) mode is vulnerable because it doesn't provide serious message confidentiality: under a given key any given plaintext block always gets encrypted to the same ciphertext block.
 - Cipher Block Chaining (CBC) with PKCS#5 padding (or PKCS#7) is vulnerable to padding oracle attacks.
- RSA encryption algorithm should be used with the recommended padding scheme (OAEP)

Also Shows Sample Code



Noncompliant Code Example

```
Cipher c0 = Cipher.getInstance("AES"); // Noncompliant: by default ECB mode is chosen

Cipher c1 = Cipher.getInstance("AES/ECB/NoPadding"); // Noncompliant: ECB doesn't provide serious message confidentiality

Cipher c3 = Cipher.getInstance("Blowfish/ECB/PKCS5Padding"); // Noncompliant: ECB doesn't provide serious message confidentiality

Cipher c4 = Cipher.getInstance("DES/ECB/PKCS5Padding"); // Noncompliant: ECB doesn't provide serious message confidentiality

Cipher c6 = Cipher.getInstance("AES/CBC/PKCS5Padding"); // Noncompliant: CBC with PKCS5 is vulnerable to oracle padding attacks
```

Compliant Solution

```
// Recommended for block ciphers
Cipher c5 = Cipher.getInstance("AES/GCM/NoPadding"); // Compliant

// Recommended for RSA
Cipher c15 = Cipher.getInstance("RSA/None/OAEPWithSHA-1AndMGF1Padding"); // Compliant
Cipher c16 = Cipher.getInstance("RSA/None/OAEPWITHSHA-256ANDMGF1PADDING"); // Compliant
```

See

- OWASP Top 10 2017 Category A6 Security Misconfiguration
- MITRE, CWE-327 Use of a Broken or Risky Cryptographic Algorithm
- CERT, MSC61-J. Do not use insecure or weak cryptographic algorithms

Both noncompliant samples AND Compliant code samples

And lots more info on each issue

Honolulu Global Requirement



- CII Website Documentation reviews:
 - Crypto Credentials Agility
 - Implement Secure Design
- One Work Item for many projects:
 - Review any Crypto Weaknesses

https://jira.onap.org/browse/REQ-443



Thank you! Q & A

