



LFN Developer & Testing Forum

ONAP Honolulu CII Badging

Tony Hansen

2021-02-03

@tonylhansen

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:
 1. Log into the CII website and check your answer
 2. If your application can say “Yes, we do that”, then click “Met”
 3. 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.

“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	clamp 2	sdc 3
	acher 1	dcaegen2	sdnc-northbound 1
	model-loader 1	collectors-	so 9
	rest-client 1	restconf 9	vfc-nfvo-driver
appc 20		music 5	svnfm-huawei 2
ccsdk	apps 2	optf cmso 12	vnfm-svnfm-nokiav2 3
	sli-adaptors 3	fgps 2	vid 2
	sli-northbound 2	has 2	vnfsdk-ves-agent 1
	sli-plugins 6	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>

The screenshot shows the SonarCloud interface for the organization 'onap'. The main header includes the SonarCloud logo, 'Explore' button, a search bar for projects and files, and a 'Log in' button. Below the header, the organization name 'Open Network Automation Platform (ONAP)' is displayed with a description 'An open source platform for d...' and a link to 'https://www.onap.org'. The 'Key' is 'onap'. Navigation tabs include 'Projects', 'Issues', 'Quality Profiles', 'Rules', and 'Quality Gates'. The 'Projects' tab is active, showing a list of 165 projects. The left sidebar contains filters for 'Quality Gate' (Passed: 150, Failed: 15) and 'Reliability' (A: 62, B: 4, C: 48, D: 13, E: 38). The main content area shows three project cards: 'aaf-authz' (Failed), 'aaf-certservice' (Passed), and 'aai-aai-common' (Passed). Each card displays various quality metrics such as Bugs, Vulnerabilities, Hotspots Reviewed, Code Smells, Coverage, and Duplications. A notification at the bottom right indicates 'Weak SSL/TLS protocols should...'.

sonarcloud Explore Log in

Open Network Automation Platform (ONAP) An open source platform for d... <https://www.onap.org> Key: onap

Projects Issues Quality Profiles Rules Quality Gates

Filters

Perspective: Overall Status Sort by: Name 165 projects

Quality Gate

Passed 150

Failed 15

Reliability (Bugs)

A 62

B 4

C 48

D 13

E 38

Security (Vulnerabilities)

A 80

B 25

C 5

D 21

E 34

aaf-authz Failed

Last analysis: January 31, 2021, 7:54 PM

29 Bugs | 263 Vulnerabilities | 0.0% Hotspots Reviewed | 3.8k Code Smells | 31.5% Coverage | 3.6% Duplications | 58k Java, XML

aaf-certservice Passed

Last analysis: February 1, 2021, 8:52 AM

2 Bugs | 0 Vulnerabilities | 0.0% Hotspots Reviewed | 71 Code Smells | 83.1% Coverage | 0.0% Duplications | 2.3k Java, XML

aai-aai-common Passed

Last analysis: February 1, 2021, 3:13 AM

34 Bugs | 19 Vulnerabilities | 0.0% Hotspots Reviewed | 1.8k Code Smells | 54.4% Coverage | Duplications | Java, XML

Weak SSL/TLS protocols should...

You Do Not Need to Login

The screenshot shows the SonarCloud web interface for the organization 'Open Network Automation Platform (ONAP)'. The browser address bar shows the URL: `sonarcloud.io/organizations/onap/projects?sort=name`. The page header includes the SonarCloud logo, an 'Explore' button, and a search bar. A red circle highlights the 'Log in' button in the top right corner.



The main content area displays a list of projects under the 'Overall Status' perspective, sorted by name. The first three projects are:


- aaf-authz** (Failed):
 - Last analysis: January 31, 2021, 7:54 PM
 - 29 Bugs (D), 263 Vulnerabilities (E), 0.0% Hotspots Reviewed (E), 3.8k Code Smells (A), 31.5% Coverage, 3.6% Duplications, 58k Java, XML (M)
- aaf-certservice** (Passed):
 - Last analysis: February 1, 2021, 8:52 AM
 - 2 Bugs (C), 0 Vulnerabilities (A), 0.0% Hotspots Reviewed (E), 71 Code Smells (A), 83.1% Coverage, 0.0% Duplications, 2.3k Java, XML (S)
- aai-aai-common** (Passed):
 - Last analysis: February 1, 2021, 3:13 AM
 - 34 Bugs (E), 19 Vulnerabilities (E), 0.0% Hotspots Reviewed (E), 1.8k Code Smells (A), 54.4% Coverage

The left sidebar contains filters for Quality Gate (Passed: 150, Failed: 15), Reliability (A-E), and Security (A-E).

Click on "Issues"

The screenshot shows the SonarCloud web interface for the ONAP organization. The browser address bar displays `sonarcloud.io/organizations/onap/projects?sort=name`. The page header includes the SonarCloud logo, an 'Explore' button, a search bar for projects and files, and a 'Log in' button. The main content area is titled 'Automation Platform (ONAP)' and includes a navigation menu with 'Issues' highlighted by a red circle. Below the navigation, there are filters for 'Quality Gate' (Passed: 150, Failed: 15) and 'Reliability' (A: 62, B: 4, C: 48, D: 13, E: 38). The 'Security' section shows 80 vulnerabilities (A: 25, B: 5, C: 21, D: 34). The main project list shows three projects: 'aaf-authz' (Failed), 'aaf-certservice' (Passed), and 'aai-aai-common' (Passed). Each project card displays various quality metrics such as Bugs, Vulnerabilities, Hotspots Reviewed, Code Smells, Coverage, and Duplications. A notification at the bottom right indicates 'Weak SSL/TLS protocols should...'.

sonarcloud  Explore  Search for projects and files... Log in








Automation Platform (ONAP)  An open source platform for d... <https://www.onap.org> Key: onap

Issues Issues Issues Profiles Rules Quality Gates








Filters

Perspective: Overall Status Sort by: Name Search by project 165 projects






aaf-authz Failed Last analysis: January 31, 2021, 7:54 PM

29  Bugs 263  Vulnerabilities 0.0%  Hotspots Reviewed 3.8k  Code Smells 31.5%  Coverage 3.6%  Duplications 58k  Java, XML

aaf-certservice Passed Last analysis: February 1, 2021, 8:52 AM

2  Bugs 0  Vulnerabilities 0.0%  Hotspots Reviewed 71  Code Smells 83.1%  Coverage 0.0%  Duplications 2.3k  Java, XML

aai-aai-common Passed Last analysis: February 1, 2021, 3:13 AM

34  Bugs 19  Vulnerabilities 0.0%  Hotspots Reviewed 1.8k  Code Smells 54.4%  Coverage Weak SSL/TLS protocols should...



Filters

Type

- Bug 3.5k
- Vulnerability 1.9k
- Code Smell 79k

Severity

- Blocker 9.5k Minor 26k
- Critical 12k Info 1.8k
- Major 35k

Resolution

Status

Security Category

Creation Date

Language

Rule

Tag

to select issues to navigate 1 / 84,614 issues 1551d effort

externalapi-nbi / pom.xml

Remove this commented out code. Why is this an issue? 2 years ago L89
 Code Smell Major Open Not assigned 5min effort misra, unused

Remove this commented out code. Why is this an issue? 2 years ago L417
 Code Smell Major Open Not assigned 5min effort misra, unused

externalapi-nbi / src/main/java/org/onap/nbi/OnapComponentsUriPaths.java

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L29
 Code Smell Minor Open Not assigned 20min effort android, cert

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L30
 Code Smell Minor Open Not assigned 20min effort android, cert

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L31
 Code Smell Minor Open Not assigned 20min effort android, cert

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L32
 Code Smell Minor Open Not assigned 20min effort Weak SSL/TLS protocols shoul...

Click on "Security Category"

sonarcloud

Explore Log in

Open Network Automation Platform (ONAP) An open source platform for d... <https://www.onap.org> Key: onap

Projects Issues Quality Profiles Rules Quality Gates

Filters

- Type
 - Bug 3.5k
 - Vulnerability 1.9k
 - Code Smell 79k
- Severity
 - Blocker 9.5k
 - Critical 12k
 - Major 35k
 - Minor 26k
 - Info 1.8k
- Resolution
 - Security Category**

externalapi-nbi / pom.xml

- Remove this commented out code. Why is this an issue? 2 years ago L89 misra, unused
 - Code Smell Major Open Not assigned 5min effort
- Remove this commented out code. Why is this an issue? 2 years ago L417 misra, unused
 - Code Smell Major Open Not assigned 5min effort

externalapi-nbi / src/main/java/org/onap/nbi/OnapComponentsUriPaths.java

- Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L29 android, cert
 - Code Smell Minor Open Not assigned 20min effort
- Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L30 android, cert
 - Code Smell Minor Open Not assigned 20min effort
- Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L31 android, cert
 - Code Smell Minor Open Not assigned 20min effort
- Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L32 Weak SSL/TLS protocols should...
 - Code Smell Minor Open Not assigned 20min effort

sonarcloud.io/organizations/onap/issues?resolved=false

sonarcloud Explore Search for projects and files... Log in

Open Network Automation Platform (ONAP) An open source platform for d... <https://www.onap.org> Key: onap

Projects Issues Quality Profiles Rules Quality Gates

Blocker	9.5k	Minor	26k
Critical	12k	Info	1.8k
Major	35k		

Resolution

Status

Security Category

- SonarSource
 - Others 84k
 - Insecure Configuration 247
 - Log Injection 218
 - Weak Cryptography 196
 - Server-Side Request Forgery (SSRF) 71
 - Path Traversal Injection 52
 - XML External Entity (XXE) 39
 - Authentication 24
 - Cross-Site Scripting (XSS) 14
 - SQL Injection 5
 - Object Injection 2
 - Command Injection 1

externalapi-nbi / pom.xml

Remove this commented out code. Why is this an issue? 2 years ago L89 Code Smell Major Open Not assigned 5min effort misra, unused

externalapi-nbi / src/main/java/org/onap/nbi/OnapComponentsUriPaths.java

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L29 Code Smell Minor Open Not assigned 20min effort android, cert

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L30 Code Smell Minor Open Not assigned 20min effort android, cert

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L31 Code Smell Minor Open Not assigned 20min effort android, cert

Refactor your code to get this URI from a customizable parameter. Why is this an issue? 2 years ago L32 Code Smell Minor Open Not assigned 20min effort Weak SSL/TLS protocols should...

Click on "Weak Cryptography"

The screenshot shows the SonarCloud interface for the Open Network Automation Platform (ONAP) project. The left sidebar contains a navigation menu with the following items:

- Projects
- Issues
- Quality Profiles
- Rules
- Quality Gates

Under the 'Issues' section, there is a 'Security Category' dropdown menu. The 'Weak Cryptography' category is highlighted with a red oval. Other categories listed include:

- Blocker (9.5k)
- Critical (12k)
- Major (35k)
- Minor (26k)
- Info (1.8k)
- SonarSource
- Others (84k)
- Log Injection (218)
- Weak Cryptography (96)
- Server-Side Request Forgery (71)
- XML External Entity (XXE) (39)
- Authentication (24)
- Cross-Site Scripting (XSS) (14)
- SQL Injection (5)
- Object Injection (2)
- Command Injection (1)

The main content area displays a list of issues for the file `externalapi-nbi / pom.xml`. The issues are:

- Remove this commented out code. Why is this an issue?** (2 years ago, L89, Code Smell, Major, Open, Not assigned, 5min effort, misra, unused)
- Remove this commented out code. Why is this an issue?** (2 years ago, L417, Code Smell, Major, Open, Not assigned, 5min effort, misra, unused)

The main content area also displays a list of issues for the file `externalapi-nbi / src/main/java/org/onap/nbi/OnapComponentsUriPaths.java`. The issues are:

- Refactor your code to get this URI from a customizable parameter. Why is this an issue?** (2 years ago, L29, Code Smell, Minor, Open, Not assigned, 20min effort, android, cert)
- Refactor your code to get this URI from a customizable parameter. Why is this an issue?** (2 years ago, L30, Code Smell, Minor, Open, Not assigned, 20min effort, android, cert)
- Refactor your code to get this URI from a customizable parameter. Why is this an issue?** (2 years ago, L31, Code Smell, Minor, Open, Not assigned, 20min effort, android, cert)
- Refactor your code to get this URI from a customizable parameter. Why is this an issue?** (2 years ago, L32, Code Smell, Minor, Open, Not assigned, 20min effort, Weak SSL/TLS protocols should...

Blocker	29	Minor	0
Critical	156	Info	0
Major	11		

Resolution

Status

Security Category SONAR ... Clear

- SonarSource WEAK CRYPTOG...
 - Others 84k
 - Insecure Configuration 247
 - Log Injection 218
 - Weak Cryptography 196
 - Server-Side Request Forgery (SSRF) 71
 - Path Traversal Injection 52
 - XML External Entity (XXE) 39
 - Authentication 24
 - Cross-Site Scripting (XSS) 14
 - SQL Injection 5
 - Object Injection 2
 - Command Injection 1

to select issues to navigate 1 / 196 issues 1d 7h effort

vnfsdk-ves-agent-vesjavaibrar... / src/.../java/evel_javaibrary/att/com/AgentMain.java

Enable server certificate validation on this SSL/TLS connection. Why is this an issue? 3 years ago L208 No tags

Vulnerability Critical Open Not assigned 5min effort

Enable server certificate validation on this SSL/TLS connection. Why is this an issue? 3 years ago L211 No tags

Vulnerability Critical Open Not assigned 5min effort

Enable server hostname verification on this SSL/TLS connection. Why is this an issue? 2 years ago L265 No tags

Vulnerability Critical Open Not assigned 5min effort

Enable server hostname verification on this SSL/TLS connection. Why is this an issue? 3 years ago L406 No tags

Vulnerability Critical Open Not assigned 5min effort

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

Use secure mode and padding scheme. Why is this an issue? 3 years ago L106 No tags

Vulnerability Blocker Open Not assigned

Use secure mode and padding scheme. Why is this an issue? 3 years ago L125 No tags

Vulnerability Blocker Open Not assigned


Weak SSL/TLS protocols shoul... x

Drilling Down

Enable server certificate validation on this SSL/TLS connection. [Why is this an issue?](#)

3 years ago ▾ L208 🔗 ⌵

 Vulnerability  Critical  Open Not assigned 5min effort


 No tags

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

Use secure mode and padding scheme. [Why is this an issue?](#)

3 years ago ▾ L106 🔗 ⌵

 Vulnerability  Blocker  Open Not assigned

 No tags

Note the Estimated Effort to Fix

Enable server certificate validation on this...
Vulnerability Critical Open Not assigned 5min effort

[Why is this an issue?](#)

3 years ago L208

No tags

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

Use secure mode and padding scheme. [Why is this an issue?](#)

3 years ago L106

Vulnerability Blocker Open Not assigned

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?](#)

Vulnerability Critical Open Not assigned 5min effort

3 years ago ▾

No tags

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

3 years ago ▾ L100

No tags

Direct Link to the Code

Enable server certificate validation on this SSL/TLS connection. [Why is this an issue?](#)

3 years ago ▾ L208 🔗 ⌵

🔒 Vulnerability 🔴 Critical 🔵 Open Not assigned 5min effort

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

Use secure mode and padding scheme. [Why is this an issue?](#)

3 years ago ▾ L106 🔗 ⌵

🔒 Vulnerability 🔴 Blocker 🔵 Open Not assigned

A View With the Code

The screenshot shows the SonarCloud web interface. At the top, the browser address bar displays the URL: `sonarcloud.io/organizations/onap/issues?open=AXGFM1LNi8tIF3n92utq&resolved=false&sonarsourceSecurity=weak-cryptography`. The SonarCloud logo and navigation menu (Explore, Search for projects and files..., Log in) are visible. The main content area is titled "Open Network Automation Platform (ONAP)" and shows a list of issues under the "Issues" tab. A specific issue is highlighted with a red border, titled "Use secure mode and padding scheme." with a "Vulnerability" severity and a "+1" count. The issue description includes a link to "Why is this an issue?". Below the issue details, a code editor shows the corresponding Java code. The code defines constants for encryption key, algorithm details, and IV block sizes, and implements an `encrypt` method. A red vertical bar on the left side of the code editor indicates the line number corresponding to the issue. A tooltip for the issue is visible over the code, showing the severity "Vulnerability", a "Blocker" status, and "3 years ago" and "L106" information.

```
69 ... private static final String AES_ENCRYPTION_KEY = "AES_ENCRYPTION_KEY";
70 ...
71 ... /**
72 ...  * Detailed definition of encryption algorithm.
73 ...  */
74 ... 1 private static final String ALGORITHM_DETAILS = ALGORITHM + "/CBC/PKCS5SPADDING";
75 ... private static final int IV_BLOCK_SIZE_IN_BITS = 128;
76 ... /**
77 ...  * An Initial Vector of 16 Bytes, so 32 Hexadecimal Chars.
78 ...  */
79 ... private static final int IV_BLOCK_SIZE_IN_BYTES = IV_BLOCK_SIZE_IN_BITS / 8;
80 ...
81 ... * @throws GeneralSecurityException In case of issue with the encryption
82 ... * @throws UnsupportedEncodingException In case of issue with the charset
83 ... * conversion
84 ... */
85 ... public static String encrypt(String value) throws GeneralSecurityException {
86 ...     Cipher cipher = Cipher.getInstance(ALGORITHM_DETAILS, "SunJCE");
87 ...
88 ...     byte[] iv = new byte[IV_BLOCK_SIZE_IN_BYTES];
89 ...     SecureRandom.getInstance("SHA1PRNG").nextBytes(iv);
90 ...     IvParameterSpec ivspec = new IvParameterSpec(iv);
91 ...     cipher.init(Cipher.ENCRYPT_MODE, SECRET_KEY_SPEC, ivspec);
92 ...     return Hex.encodeHexString(ArrayUtils.addAll(iv, cipher.doFinal(value.getBytes(Charsets.UTF_8))));
93 ... }
94 ...
95 ... /**
```

Each Jira ticket will go directly to this view

Click “Why is this an issue?”

The screenshot shows the SonarCloud web interface for the Open Network Automation Platform (ONAP) project. The main content area displays a code snippet from `...a/org/onap/clamp/clds/util/CryptoUtils.java`. The code defines constants for encryption and implements an `encrypt` method. A red vertical bar on the left side of the code editor indicates the location of an issue.

The issue is titled "Use secure mode and padding scheme" and is categorized as a "Vulnerability" with a severity of "+1". The issue tooltip, which is highlighted with a red circle, contains the text "Why is this an issue?". Other details in the tooltip include "3 years ago", "L106", and "No tags".

```
69 -- private static final String AES_ENCRYPTION_KEY = "AES_ENCRYPTION_KEY";
70 --
71 -- /**
72 --  * Detailed definition of encryption algorithm.
73 --  */
74 -- 1 private static final String ALGORITHM_DETAILS = ALGORITHM + "/CBC/PKCS5PADDING";
75 -- private static final int IV_BLOCK_SIZE_IN_BITS = 128;
76 -- /**
77 --  * An Initial Vector of 16 Bytes, so 32 Hexadecimal Chars.
78 --  */
79 -- private static final int IV_BLOCK_SIZE_IN_BYTES = IV_BLOCK_SIZE_IN_BITS / 8;
80 --
81 --
82 --
83 --
84 --
85 --
86 --
87 --
88 --
89 --
90 --
91 --
92 --
93 --
94 --
95 --
96 --
97 --
98 --
99 --
100 --
101 -- * @throws GeneralSecurityException In case of issue with the encryption
102 -- * @throws UnsupportedEncodingException In case of issue with the charset
103 -- * conversion
104 -- */
105 -- public static String encrypt(String value) throws GeneralSecurityException {
106 --     Cipher cipher = Cipher.getInstance(ALGORITHM_DETAILS, "SunJCE");
107 --
108 --     byte[] iv = new byte[IV_BLOCK_SIZE_IN_BYTES];
109 --     SecureRandom.getInstance("SHA1PRNG").nextBytes(iv);
110 --     IvParameterSpec ivspec = new IvParameterSpec(iv);
111 --     cipher.init(Cipher.ENCRYPT_MODE, SECRET_KEY_SPEC, ivspec);
112 --     return Hex.encodeHexString(ArrayUtils.addAll(iv, cipher.doFinal(value.getBytes(Charsets.UTF_8))));
113 -- }
114 -- /**
```

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

java:S5542

Vulnerability **Blocker** Main sources cert, cwe, owasp-a3, owasp-a6, priva... 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
```

Both noncompliant samples AND
Compliant code samples

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

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



OLF NETWORKING

LFN Developer & Testing Forum