SECCOM CII Badging Focus Topics

Today's Focus Topic: Crypto used network

SECCOM

2019/8/26

Why are we doing this?

Thank you to all of the projects that ***have*** already answered this question

Unfortunately, only half of the projects have answered this question.

Bottom line: Our job is to get ONAP projects to verify and/or improve the security of their code. Getting the silver star or gold star from the CII badge is truly secondary.

This is one of a set of “focused CII security issues”

The CII question

The software produced by the project SHOULD/MUST support secure protocols for all of its network communications, such as SSHv2 or later, TLS1.2 or later (HTTPS), IPsec, SFTP, and SNMPv3. Insecure protocols such as FTP, HTTP, telnet, SSLv3 or earlier, and SSHv1 SHOULD/MUST be ***disabled by default***, and only enabled if the user specifically configures it.

If the software produced by the project does not support network communications, select 'not applicable' (N/A).

Intro

- This question is about ***incoming*** connections.
- This question is about how insecure protocols, or insecure versions of some protocols, are enabled.
- The insecure protocols/versions must not be enabled by default.
- The insecure protocols/versions can be enabled through configuration.

PTL Effort

- Check that your applications do not turn on insecure protocols or versions ***by default***, for example, incoming HTTP is NOT enabled as delivered.
- Having an option to switch ***between*** secure and insecure protocols is not correct and does not meet the criteria. (The secure version must always be enabled.)
- Having an option to ***turn on*** the secure version is backwards and does not meet the criteria.

You may delegate the checking of the code.

How to answer the CII question

- For *each* incoming network connection supported by your application:
- Does it enable one of the insecure protocols or versions by default?
- Is a variable needed to turn on the secure protocol, compared to turning on the insecure protocol?
- Is the secure protocol disabled if the insecure protocol is enabled? (Is it a toggle?)
- Is an insecure protocol accidently enabled if something is wrong with something needed for the secure protocol to work? (e.g. a missing key)

(***no*** answers are good)

How to answer, continued

If there are no incoming connections:

- Click (N/A)
- In the description, enter the date (e.g., [2019/08/26]) and an indication why N/A was appropriate

If NO for all incoming connections:

- Click (Met)
- In the description, enter the date (e.g., [2019/08/26]) and an indication why (Met) is appropriate

If some of the answers are YES (you ***have*** some insecure protocols/versions enabled by default):

- Click (Unmet)
- In the description, enter the date (e.g., [2019/08/26]) and a description where something was not met.
- File JIRA tickets for each issue that needs resolution.
- In the description, enter the date and document which pieces meet or do not meet the criteria.
- You can also document which pieces DO meet the criteria, if there is a mixture.

Where to answer

This part should take about 5 minutes

- Go to https://bestpractices.coreinfrastructure.org
- Click Projects
- Search for your project
- Click Login (at the top)
- Click Edit (at the top)
- Click the button that says [silver]
- Scroll to the bottom, click [v] Security
- Search for “crypto_used_network”
- Fill in your answers
- Click one of the green buttons [Save (and continue)] or [Submit (and exit)]

Thank you

- That’s all