Network App Certification Report: FogusNetApp

Date: 20/11/2023

CERTIFICATION REPORT EXECUTIVE SUMMARY

This Certification Report contains the results of the Certification process executed over the Network App **FogusNetApp** version **4.0**

Certification triggered by JORGE / id02658
Repo used for Certification: **https://github.com/EVOLVED-5G/FogusNetApp**
Branch used for Certification: evolved5g
Last commit ID: d2885d0ec48c9b78f165753242612f7557c08df6
Environment used: **kubernetes-cosmote**
Build number at Jenkins: 157
Network App deploy time KPI: **24 seconds**
Total Certification time: **57 Min**

The result of the Certification Process over the Network App **FogusNetApp** has been: **SUCCESS**

The individual result of the certifications test is displayed in the following table:

Step	Step Name	Result
0	PLATFORM ASSESSMENT	SUCCESS
1	SOURCE CODE STATIC ANALYSIS	SUCCESS
2	SOURCE CODE SECURITY ANALYSIS	SUCCESS
3	SOURCE CODE SECRETS LEAKAGE	SUCCESS
4	NETWORK APP BUILD AND PORT CHECK	SUCCESS
5	IMAGE SECURITY ANALYSIS	SUCCESS
6	DEPLOY FOGUSNETAPP NETWORK APP	SUCCESS
7	USE OF 5G APIS	SUCCESS
8	NETWORK APP KPIS	SUCCESS
9	OPEN SOURCE LICENSES REPORT	SUCCESS

Congratulations your Network App FogusNetApp has been certified

In the following pages, we provide details of the tests executed and the results.

PLATFORM ASSESSMENT

This step shows results of platform assessment measures.

TSN experiments

Delay and jitter experiments were carried out using predefined test case templates: UMA_TSN_OWD and UMA_TSN_Jitter, which corresponds to the evaluation of the Downlink One-Way Delay (OWD) and jitter on the TSN over 5G architecture, respectively.

One-Way Delay (ns) - TSN scenario

This test evaluates the One-Way Delay (OWD) of a TSN over 5G SA network. The main goal of this test is to assess the end-to-end delay of the TSN over 5G infrastructure that lays on the UMA platform.

Indicator	Value	Confidence Interval
25% Percentile	5636150.39	235867.39
5% Percentile	5485145.36	252703.17
75% Percentile	6171831.91	367331.07
95% Percentile	6482334.64	344746.05
Max	7455185.73	1105994.33
Mean	5918610.89	268066.77
Median	5899707.63	308110.15
Min	5336491.35	204376.80
Standard Deviation	387955.97	124961.22

Jitter (ns) - TSN scenario

This test evaluates the Jitter of a TSN over 5G SA network. The main goal of this test is to assess the end-to-end jitter of the TSN over 5G infrastructure that lays on the UMA platform.

Indicator	Value	Confidence Interval
25% Percentile	922242.65	202034.36
5% Percentile	712654.77	137255.15
75% Percentile	1391197.28	222058.36
95% Percentile	1622248.64	155953.38
Max	1988893.58	171223.24
Mean	1126875.32	167678.41
Median	1037233.30	213507.84
Min	606141.43	133045.07
Standard Deviation	331972.47	76597.79

Platform KPIs

This experiments over platform shows the usual measures at environment under test like Delay, Jitter and Throughput of traffic and also percent of total memory used.

Kpi type Platform

KPI Name	Min	Max	Mean	Median	Standar Deviation	Description
Used RAM (%)	38.11	38.37	38.23	38.23	0.07	Amount of memory currently storing useful data.
Jitter (ms)	0.00	0.00	0.00	0.00	0.00	Slight irregular movement, variation, or unsteadiness, especially in an electrical signal or electronic device.
Throughput (Mbps)	391.33	1159.67	928.63	961.50	143.40	The amount of material or items passing through a system or process.
Delay (ms)	7.10	114.00	16.54	14.77	13.23	A period of time by which something is late or postponed.

SOURCE CODE STATIC ANALYSIS

Test Description: SonarQube is a Code Quality Assurance tool that collects and analyzes source code, and provides reports for the code quality of your project. It combines static and dynamic analysis tools and enables quality to be measured continually over time.

Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: d2885d0ec48c9b78f165753242612f7557c08df6

The Source Code analysis has been performed using SonarQube version "8.3.0.34182"

Scan of fogusnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	9
major	28
minor	19

Good work. Network App code does not have any blocker issues.

The information for critical, major and minor issues can be found in the following link:
https://sq.mobilesandbox.cloud:9000/dashboard?id=Evolved5g-fogusnetapp-evolved5g

SOURCE CODE SECURITY ANALYSIS

Test Description: This test detects vulnerabilities in the source code of the Network App repo.
Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: d2885d0ec48c9b78f165753242612f7557c08df6

The security scan has been performed using Trivy version 0.35.0

Scan of repo: FogusNetApp

Good work. No vulnerabilities found.

Information about high, medium, low and unknown issues can be found in the following link: https://github.com/EVOLVED-5G/FogusNetApp/wiki/Telefonica-Evolved5g-FogusNetApp

SOURCE CODE SECRETS LEAKAGE

Test Description: This test analyse the source code and detects secrets exposed.
Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: d2885d0ec48c9b78f165753242612f7557c08df6

Summary

Rule	Number of secrets leaked
Exposed Domains	12

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Exposed Domains	image: dockerhub.hi.inet	fogus/templates/netappdjango-deployment.yaml (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/fogus/templates/netappdjango-deployment.yaml#L34-L34)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	image: dockerhub.hi.inet	fogus/templates/dbnetapp-deployment.yaml (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/fogus/templates/dbnetapp-deployment.yaml#L35-L35)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	- image: dockerhub.hi.inet	fogus/templates/netappfe-deployment.yaml (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/fogus/templates/netappfe-deployment.yaml#L28-L28)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-29 12:43
low	Exposed Domains	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-FogusNetApp/blob/699cd0dc9483f99e33e4340884d814dfb8bc0821/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-29 12:43

The Source Code Secrets Leakage scan stage has been completed successfuly.

More information can be found in the following link: https://github.com/EVOLVED-5G/FogusNetApp/wiki/secrets-Telefonica-Evolved5g-FogusNetApp

NETWORK APP BUILD AND PORT CHECK

This step build needed images for current Network App, checks ports exposed and publish docker images.

https://github.com/EVOLVED-5G/FogusNetApp Network apps are composed of the following services:

- fogusnetapp-netappdjango
- fogusnetapp-netappfe
- fogusnetapp-netapppostgres

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
fogusnetapp-netappdjango		
	8000	OK
fogusnetapp-netappfe		
	4200	OK
fogusnetapp-netapppostgres		

Publication of Network App docker images

Urls of Images published:

Image: **fogusnetapp-netappdjango**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/certification/fogusnetapp/fogusnetapp-netappdjango:4.0
- dockerhub.hi.inet/evolved-5g/certification/fogusnetapp/fogusnetapp-netappdjango:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gcertification:fogusnetapp-netappdjango-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gcertification:fogusnetapp-netappdjango-latest

Image: **fogusnetapp-netappfe**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/certification/fogusnetapp/fogusnetapp-netappfe:4.0
- dockerhub.hi.inet/evolved-5g/certification/fogusnetapp/fogusnetapp-netappfe:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gcertification:fogusnetapp-netappfe-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gcertification:fogusnetapp-netappfe-latest

Image: **fogusnetapp-netapppostgres**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/certification/fogusnetapp/fogusnetapp-netapppostgres:4.0
- dockerhub.hi.inet/evolved-5g/certification/fogusnetapp/fogusnetapp-netapppostgres:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gcertification:fogusnetapp-netapppostgres-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gcertification:fogusnetapp-netapppostgres-latest

IMAGE SECURITY ANALYSIS OF netappdjango 1 / 3

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **netappdjango**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	60
MEDIUM	221
LOW	505
UNKNOWN	2

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-28531 (https://nvd.nist.gov/vuln/detail/CVE-2023-28531)	openssh: smartcard keys to ssh-agent without the intended per-hop destination constraints.	openssh-client	1:9.2p1-2+deb12u1	
CRITICAL	CVE-2023-45853 (https://nvd.nist.gov/vuln/detail/CVE-2023-45853)	zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6	zlib1g	1:1.2.13.dfsg-1	
CRITICAL	CVE-2023-45853 (https://nvd.nist.gov/vuln/detail/CVE-2023-45853)	zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6	zlib1g-dev	1:1.2.13.dfsg-1	

The Docker Images Security Analysis has been completed successfuly
Information about high, medium, low and unknown issues can be found in the following link: https://github.com/EVOLVED-5G/FogusNetApp/wiki/dockerhub.hi.inet-evolved-5g-certification-fogusnetapp-fogusnetapp-netappdjango

IMAGE SECURITY ANALYSIS OF netappfe 2 / 3

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **netappfe**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
CRITICAL	61
HIGH	721
MEDIUM	1058
LOW	1403
UNKNOWN	41

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	curl	7.64.0-4+deb10u2	7.64.0-4+deb10u4
CRITICAL	CVE-2022-23521 (https://nvd.nist.gov/vuln/detail/CVE-2022-23521)	git: gitattributes parsing integer overflow	git	1:2.20.1-2+deb10u3	1:2.20.1-2+deb10u7
CRITICAL	CVE-2022-41903 (https://nvd.nist.gov/vuln/detail/CVE-2022-41903)	git: Heap overflow in `git archive`, `git log --format` leading to RCE	git	1:2.20.1-2+deb10u3	1:2.20.1-2+deb10u7
CRITICAL	CVE-2022-23521 (https://nvd.nist.gov/vuln/detail/CVE-2022-23521)	git: gitattributes parsing integer overflow	git-man	1:2.20.1-2+deb10u3	1:2.20.1-2+deb10u7
CRITICAL	CVE-2022-41903 (https://nvd.nist.gov/vuln/detail/CVE-2022-41903)	git: Heap overflow in `git archive`, `git log --format` leading to RCE	git-man	1:2.20.1-2+deb10u3	1:2.20.1-2+deb10u7
CRITICAL	CVE-2021-33574 (https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	mq_notify does not handle separately allocated thread attributes	libc-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-35942 (https://nvd.nist.gov/vuln/detail/CVE-2021-35942)	Arbitrary read in wordexp()	libc-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23218 (https://nvd.nist.gov/vuln/detail/CVE-2022-23218)	Stack-based buffer overflow in svcunix_create via long pathnames	libc-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23219 (https://nvd.nist.gov/vuln/detail/CVE-2022-23219)	Stack-based buffer overflow in sunrpc clnt_create via a long pathname	libc-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-33574 (https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	mq_notify does not handle separately allocated thread attributes	libc-dev-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-35942 (https://nvd.nist.gov/vuln/detail/CVE-2021-35942)	Arbitrary read in wordexp()	libc-dev-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23218 (https://nvd.nist.gov/vuln/detail/CVE-2022-23218)	Stack-based buffer overflow in svcunix_create via long pathnames	libc-dev-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23219 (https://nvd.nist.gov/vuln/detail/CVE-2022-23219)	Stack-based buffer overflow in sunrpc clnt_create via a long pathname	libc-dev-bin	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-33574 (https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	mq_notify does not handle separately allocated thread attributes	libc6	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-35942 (https://nvd.nist.gov/vuln/detail/CVE-2021-35942)	Arbitrary read in wordexp()	libc6	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23218 (https://nvd.nist.gov/vuln/detail/CVE-2022-23218)	Stack-based buffer overflow in svcunix_create via long pathnames	libc6	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23219 (https://nvd.nist.gov/vuln/detail/CVE-2022-23219)	Stack-based buffer overflow in sunrpc clnt_create via a long pathname	libc6	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-33574 (https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	mq_notify does not handle separately allocated thread attributes	libc6-dev	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2021-35942 (https://nvd.nist.gov/vuln/detail/CVE-2021-35942)	Arbitrary read in wordexp()	libc6-dev	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23218 (https://nvd.nist.gov/vuln/detail/CVE-2022-23218)	Stack-based buffer overflow in svcunix_create via long pathnames	libc6-dev	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-23219 (https://nvd.nist.gov/vuln/detail/CVE-2022-23219)	Stack-based buffer overflow in sunrpc clnt_create via a long pathname	libc6-dev	2.28-10+deb10u1	2.28-10+deb10u2
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	libcurl3-gnutls	7.64.0-4+deb10u2	7.64.0-4+deb10u4
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	libcurl4	7.64.0-4+deb10u2	7.64.0-4+deb10u4
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	libcurl4-openssl-dev	7.64.0-4+deb10u2	7.64.0-4+deb10u4
CRITICAL	CVE-2019-8457 (https://nvd.nist.gov/vuln/detail/CVE-2019-8457)	heap out-of-bound read in function rtreenode()	libdb5.3	5.3.28+dfsg1-0.5	
	CVE-2019-8457				

CRITICAL	(https://nvd.nist.gov/vuln/detail/CVE-2019-8457)	heap out-of-bound read in function rtreenode()	libdb5.3-dev	5.3.28+dfsg1-0.5	
CRITICAL	CVE-2022-27404 (https://nvd.nist.gov/vuln/detail/CVE-2022-27404)	Buffer overflow in sfnt_init_face	libfreetype6	2.9.1-3+deb10u2	2.9.1-3+deb10u3
CRITICAL	CVE-2022-27404 (https://nvd.nist.gov/vuln/detail/CVE-2022-27404)	Buffer overflow in sfnt_init_face	libfreetype6-dev	2.9.1-3+deb10u2	2.9.1-3+deb10u3
CRITICAL	CVE-2022-3515 (https://nvd.nist.gov/vuln/detail/CVE-2022-3515)	libksba: integer overflow may lead to remote code execution	libksba8	1.3.5-2	1.3.5-2+deb10u1
CRITICAL	CVE-2022-47629 (https://nvd.nist.gov/vuln/detail/CVE-2022-47629)	libksba: integer overflow to code execution	libksba8	1.3.5-2	1.3.5-2+deb10u2
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	pcre2: Out-of-bounds read in compile_xclass_matchingpath in pcre2_jit_compile.c	libpcre2-8-0	10.32-5	10.32-5+deb10u1
CRITICAL	CVE-2022-1587 (https://nvd.nist.gov/vuln/detail/CVE-2022-1587)	pcre2: Out-of-bounds read in get_recurse_data_length in pcre2_jit_compile.c	libpcre2-8-0	10.32-5	10.32-5+deb10u1
CRITICAL	CVE-2021-3177 (https://nvd.nist.gov/vuln/detail/CVE-2021-3177)	Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c	libpython2.7-minimal	2.7.16-2+deb10u1	2.7.16-2+deb10u2
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	libpython2.7-minimal	2.7.16-2+deb10u1	2.7.16-2+deb10u3
CRITICAL	CVE-2021-3177 (https://nvd.nist.gov/vuln/detail/CVE-2021-3177)	Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c	libpython2.7-stdlib	2.7.16-2+deb10u1	2.7.16-2+deb10u2
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	libpython2.7-stdlib	2.7.16-2+deb10u1	2.7.16-2+deb10u3
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	libpython3.7-minimal	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	libpython3.7-minimal	3.7.3-2+deb10u3	3.7.3-2+deb10u6
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	libpython3.7-stdlib	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	libpython3.7-stdlib	3.7.3-2+deb10u3	3.7.3-2+deb10u6
CRITICAL	CVE-2020-35527 (https://nvd.nist.gov/vuln/detail/CVE-2020-35527)	Out of bounds access during table rename	libsqlite3-0	3.27.2-3+deb10u1	3.27.2-3+deb10u2
CRITICAL	CVE-2020-35527 (https://nvd.nist.gov/vuln/detail/CVE-2020-35527)	Out of bounds access during table rename	libsqlite3-dev	3.27.2-3+deb10u1	3.27.2-3+deb10u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	libssl-dev	1.1.1n-0+deb10u2	1.1.1n-0+deb10u3
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	libssl1.1	1.1.1n-0+deb10u2	1.1.1n-0+deb10u3
CRITICAL	CVE-2021-46848 (https://nvd.nist.gov/vuln/detail/CVE-2021-46848)	Out-of-bound access in ETYPE_OK	libtasn1-6	4.13-3	4.13-3+deb10u1
CRITICAL	CVE-2021-46848 (https://nvd.nist.gov/vuln/detail/CVE-2021-46848)	Out-of-bound access in ETYPE_OK	libtasn1-6-dev	4.13-3	4.13-3+deb10u1
CRITICAL	CVE-2023-45871 (https://nvd.nist.gov/vuln/detail/CVE-2023-45871)	kernel: IGB driver inadequate buffer size for frames larger than MTU	linux-libc-dev	4.19.235-1	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:7.9p1-10+deb10u2	1:7.9p1-10+deb10u3
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	openssl	1.1.1n-0+deb10u2	1.1.1n-0+deb10u3
CRITICAL	CVE-2021-3177 (https://nvd.nist.gov/vuln/detail/CVE-2021-3177)	Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u2
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u3
CRITICAL	CVE-2021-3177 (https://nvd.nist.gov/vuln/detail/CVE-2021-3177)	Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c	python2.7-minimal	2.7.16-2+deb10u1	2.7.16-2+deb10u2
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	python2.7-minimal	2.7.16-2+deb10u1	2.7.16-2+deb10u3
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	python3.7	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	python3.7	3.7.3-2+deb10u3	3.7.3-2+deb10u6
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	python3.7-minimal	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	python: XML External Entity in XML processing plistlib module	python3.7-minimal	3.7.3-2+deb10u3	3.7.3-2+deb10u6
CRITICAL	CVE-2022-37434 (https://nvd.nist.gov/vuln/detail/CVE-2022-37434)	heap-based buffer over-read and overflow in inflate() in inflate.c via a large gzip header extra fie	zlib1g	1:1.2.11.dfsg-1+deb10u1	1:1.2.11.dfsg-1+deb10u2
CRITICAL	CVE-2023-45853 (https://nvd.nist.gov/vuln/detail/CVE-2023-45853)	zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6	zlib1g	1:1.2.11.dfsg-1+deb10u1	
CRITICAL	CVE-2022-37434 (https://nvd.nist.gov/vuln/detail/CVE-2022-37434)	heap-based buffer over-read and overflow in inflate() in inflate.c via a large gzip header extra fie	zlib1g-dev	1:1.2.11.dfsg-1+deb10u1	1:1.2.11.dfsg-1+deb10u2
CRITICAL	CVE-2023-45853 (https://nvd.nist.gov/vuln/detail/CVE-2023-45853)	zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6	zlib1g-dev	1:1.2.11.dfsg-1+deb10u1	

The Docker Images Security Analysis has been completed successfuly
Information about high, medium, low and unknown issues can be found in the following link: https://github.com/EVOLVED-5G/FogusNetApp/wiki/dockerhub.hi.inet-evolved-5g-certification-fogusnetapp-fogusnetapp-netappfe

IMAGE SECURITY ANALYSIS OF netapppostgres 3 / 3

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **netapppostgres**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	36
MEDIUM	16
LOW	48

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2019-12900 (https://nvd.nist.gov/vuln/detail/CVE-2019-12900)	bzip2: out-of-bounds write in function BZ2_decompress	libbz2-1.0	1.0.6-8.1	
CRITICAL	CVE-2019-8457 (https://nvd.nist.gov/vuln/detail/CVE-2019-8457)	heap out-of-bound read in function rtreenode()	libdb5.3	5.3.28-12+deb9u1	
CRITICAL	CVE-2019-8457 (https://nvd.nist.gov/vuln/detail/CVE-2019-8457)	heap out-of-bound read in function rtreenode()	libsqlite3-0	3.16.2-5+deb9u3	

The Docker Images Security Analysis has been completed successfuly
Information about high, medium, low and unknown issues can be found in the following link: https://github.com/EVOLVED-5G/FogusNetApp/wiki/dockerhub.hi.inet-evolved-5g-certification-fogusnetapp-fogusnetapp-netapppostgres

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **FogusNetApp** version **4.0**

Repo used for Validation: **https://github.com/EVOLVED-5G/FogusNetApp**
Branch used for Validation: evolved5g
Last commit ID: d2885d0ec48c9b78f165753242612f7557c08df6
Environment used: **kubernetes-cosmote**
Build number at Jenkins: 157

The individual result of the certification tests are displayed in the following table:

Name	**Result**
ONBOARDING NETWORKAPP TO CAPIF	SUCCESS
DISCOVER NEF APIS FROM CAPIF	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-monitoring-event/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

NETWORK APP KPIS

This section will show all **FogusNetApp** Network Application with version **4.0** related KPIs.

Network App Namespace KPIs

At this section the KPIs are related with k8s environment. Here we can find CPU and Memory usage rate from network app deployment respect to the base k8s nodes total capacity.

Host	Cpu(%)	Memory(%)
evolvednode02	0.57	2.81
evolvednode01	0.18	3.10

CPU (%): The percentage of the host's CPU the container is using.
Memory (%): The percentage of the host's Memory the container is using.

Network App Pods KPIs

At this section the KPIs are related with container deployed of the Network App under test.

Service	Memory Usage(%)	Net I/O(Bytes)	Mem Failures(Times)	Block I/O(Blocks)
django	1.28	0.00	-	0.00
fe	0.72	0.00	-	0.00
dbnetapp	0.46	0.00	-	0.00

Memory Usage(%): The total memory the container is using / the total amount of memory it is allowed to use.
Net I/O (Bytes): The amount of data the container has received and sent over its network interface.
Mem Failures (Times): Tracks the number of times a container has experienced an out-of-memorv (OOM) event.
Block I/O (Blocks): The amount of data the container has written to and read from block devices on the host.

OPEN SOURCE LICENSES REPORT

Test Description: This test identifies the required licenses used in the Network App .
Network App repository used for the analysis: https://github.com/EVOLVED-5G/FogusNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: d2885d0ec48c9b78f165753242612f7557c08df6

Licenses introduce a varying degree of conditions to be fulfilled for using the licensed software. Open Source licenses gives indeed many freedoms, but seldom completely unconditionally:

- Almost all licenses require you to attribute the distributed software with a copyright and a permission notice, sometimes in addition with the entire license text.
- Some licenses require you to publish the source code as well, which add work to ensure that you are in compliance with the license.
- Some licenses add rights and conditions beyond the copyright, suchs as on patents, trademarks, data, and privacy which may make it more difficult to altogether achieve compliance of a license.
- And to complicate things even further, some Open Source licenses have conditions which makes them incompatible with other Open Source licenses. This is most notably with the GPL license.

The licenses scan has been performed using licensecheck.

- Strong copyleft license requires that other code that is used for adding, enhancing, and/or modifying the original work also must inherit all the original work’s license requirements such as to make the code publicly available.
- Weak copyleft license only requires that the source code of the original or modified work is made publicly available, other code that is used together with the work does not necessarily inherit the original work’s license requirements.

Licenses Summary Results

License Name	Dependencies
BSD LICENSE	10
MIT LICENSE	13
APACHE SOFTWARE LICENSE	7
MOZILLA PUBLIC LICENSE 2.0 (MPL 2.0)	1
GNU LESSER GENERAL PUBLIC LICENSE V2 OR LATER (LGPLV2+)	1
APACHE SOFTWARE LICENSE;; BSD LICENSE	1
GNU LIBRARY OR LESSER GENERAL PUBLIC LICENSE (LGPL)	1
PYTHON SOFTWARE FOUNDATION LICENSE	1

Dependencies Results

Compatible	Package	Version	License
✔	Click	7.0	BSD LICENSE
✔	Django	4.2.7	BSD LICENSE
✔	PyJWT	1.7.1	MIT LICENSE
✔	Sphinx	7.2.6	BSD LICENSE
✔	asgiref	3.7.2	BSD LICENSE
✔	backports.zoneinfo	0.2.1	APACHE SOFTWARE LICENSE
✔	build	1.0.3	MIT LICENSE
✔	certifi	2019.11.28	MOZILLA PUBLIC LICENSE 2.0 (MPL 2.0)
✔	charset-normalizer	3.1.0	MIT LICENSE
✔	configparser	6.0.0	MIT LICENSE
✔	cookiecutter	2.4.0	BSD LICENSE
✔	coverage	7.3.2	APACHE SOFTWARE LICENSE
✔	django-cors-headers	4.3.0	MIT LICENSE
✔	django-extensions	3.2.3	MIT LICENSE
✔	django-shell-plus	1.1.7	BSD LICENSE
✔	djangorestframework	3.14.0	BSD LICENSE
✔	evolved5g	1.0.13	APACHE SOFTWARE LICENSE
✔	flake8	6.1.0	MIT LICENSE
✔	idna	2.8	BSD LICENSE
✔	invoke	2.2.0	BSD LICENSE
✔	mariadb	1.1.8	GNU LESSER GENERAL PUBLIC LICENSE V2 OR LATER (LGPLV2+)
✔	packaging	23.2	APACHE SOFTWARE LICENSE;; BSD LICENSE
✔	psycopg2	2.9.9	GNU LIBRARY OR LESSER GENERAL PUBLIC LICENSE (LGPL)
✔	pyOpenSSL	19.0.0	APACHE SOFTWARE LICENSE
✔	pytest	7.4.3	MIT LICENSE
✔	pytest-cov	4.1.0	MIT LICENSE

✔	pytz	2023.3.post1	MIT LICENSE
✔	requests	2.31.0	APACHE SOFTWARE LICENSE
✔	six	1.14.0	MIT LICENSE
✔	sqlparse	0.4.4	BSD LICENSE
✔	typing_extensions	4.8.0	PYTHON SOFTWARE FOUNDATION LICENSE
✔	tzdata	2023.3	APACHE SOFTWARE LICENSE
✔	urllib3	1.26.15	MIT LICENSE
✔	watchdog	3.0.0	APACHE SOFTWARE LICENSE
✔	wheel	0.34.2	MIT LICENSE

Fingerprint

Network Application: FogusNetApp

Version: 4.0

Certification pipeline generate this fingerprint to sign this network application.

After a success certification process, network application can be uploaded to marketplace (https://marketplace.evolved-5g.eu/).

Marketplace will check fingerprint to validate the network application at registration process.

8e3bfc39-7e44-4084-9c54-4d444e61b146

evolved 5G