EXPERIMENTATION AND VALIDATION OPENNESS FOR LONGTERM
EVOLUTION OF VERTICAL INDUSTRIES IN 5G ERA AND BEYOND
[H2020 - Grant Agreement No.101016608]

Deliverable D5.5

NetApps Validation and onboarding to Open Repository (final)

Editor George Makropoulos (NCSRD)

Contributors (NCSRD), (TID), (ATOS), (INTRA), (COS), (MAG), (IMM), (GMI), (INF), (CAF), (ININ), (ZORT), (UMA), (8BELLS), (FOG), (IQBT), (PAL), UML)

Version 1.0

Date November 3rd, 2023

Distribution PUBLIC (PU)

DISCLAIMER

This document contains information, which is proprietary to the EVOLVED-5G ("Experimentation and Validation Openness for Longterm evolution of Vertical inDustries in 5G era and beyond) Consortium that is subject to the rights and obligations and to the terms and conditions applicable to the Grant Agreement number: 101016608. The action of the EVOLVED-5G Consortium is funded by the European Commission.

Neither this document nor the information contained herein shall be used, copied, duplicated, reproduced, modified or communicated by any means to any third party, in whole or in parts, except with prior written consent of the EVOLVED-5G Consortium. In such case, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. In the event of infringement, the consortium reserves the right to take any legal action it deems appropriate.

This document reflects only the authors' view and does necessarily reflect the view of the European Commission. Neither the EVOLVED-5G Consortium as a whole, nor a certain party of the EVOLVED-5G Consortium warrant that the information contained in this document is suitable for use, nor that the use of the information is accurate or free from risk and accepts no liability for loss or damage suffered by any person using this information.

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

REVISION HISTORY

Revision	*Date*	*Responsible*	*Comment*
0.1	*30th August*	*NCSRD*	*1ST Draft*
0.2	*10th September*	*NCSRD*	*2ND Draft*
0.3	*20th September*	*NCSRD*	*3rd Draft*
0.4	*30th September*	*NCSRD, TID, SMEs,*	*4TH Draft*
0.5	*5th October*	*NCSRD, TID,*	*Finalisation of contributions*
0.8	*15th October*	*NCSRD*	*Final edits*
0.9	*25th October*	*NCSRD, TID, UMA*	*Final draft for internal review*
1.0	*30th October*	*NCSRD, TID*	*Final version*

LIST OF AUTHORS

Partner ACRONYM	Partner FULL NAME	Name & Surname
NCSRD	NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"	George Makropoulos Dimitrios Fragkos Harilaos Koumaras Ioannis Manolopoulos Dimitris Kyriazanos
TID	TELEFONICA INVESTIGACIÓN Y DESARROLLO	Javier Garcia David Artunedo Jorge Moratinos
INTRA	NETCOMPANY INTRASOFT SA	Angela Dimitriou
IMM	IMMERSION	Charles Bailly
GMI	GMI AERO	Marc-Olivier Sauer George Kanterakis
INF	INFOLYSIS P.C	Christos Sakkas Konstantinos Fragkos George Theodoropoulos
CAFA	CAFA TECH OU	Märten Rannu Tanle Järvet
ININ	INTERNET INSTITUTE, COMMUNICATIONS SOLUTIONS AND CONSULTING LTD	Luka Korsic Jaka Cijan Rudolf Susnik
ZORTENET	ZORTENET P.C.	Akis Kourtis, Andreas Oikonomakis, George Xilouris
UMA	UNIVERSIDAD DE MÁLAGA	Bruno García Rafael López
8BELLS	EIGHT BELLS LTD	George Kontopoulos Vasilis Pasios
FOGUS	FOGUS INNOVATIONS & SERVICES	Dimitris Tsolkas Anastasios-Stavros Charismiadis Nikos Passas
IQBT	INQBIT INNOVATIONS SRL	Stylianou Ioannis, Eleni Argyriou
PAL	PAL ROBOTICS SL	Thomas Peyrucain
UML	UNMANNED SYSTEMS LIMITED	Bianca Bendris

GLOSSARY

Abbreviations-Acronym	*Description*
3GPP	3rd Generation Partnership Project
AWS	Amazon Web Services
API	Application Programming Interface
CAPIF	Common API Framework
CI/CD	Continuous Integration / Continuous Development
CPU	Central Processing Unit
KPI	Data Consistency KPI
ELCM	Experiment Life Cycle Manager
FoF	Factory of the Future
IaaC	Infrastructure as Code
IAM	Identity and Access Management
IEM	Interaction of Employees and Machines
IIoT	Industrial Internet of Things
KPI	Key Performance Indicator
NEF	Network Exposure Function
Network App	Network Application
PLI	Production Line Infrastructure
QoS	Quality of Service
REST	REpresentational State Transfer
RBAC	Role-based policy
SEC	Security Guarantees and risk Analysis
SIEM	Security Information and Event Management
SME	Small Medium Enterprise
vApp	Vertical Application
VM	Virtual Machine
VNF	Virtual Network Function
VPN	Virtual Private Network

EXECUTIVE SUMMARY

EVOLVED-5G responds to the 5G PPP ICT-41-2020 5G innovations for verticals with third party services call, whose main goal is to deliver enhanced experimentation facilities on top of which third party experimenters (e.g., SMEs or any service provider and target vertical users) will have the opportunity to test their applications. The EVOLVED-5G project realises this vision by encouraging the creation of a Network App ecosystem revolving around a 5G facility which provides the tools and processes for the development, verification, validation, and certification of Network Apps as well as their smooth running on top of actual 5G network infrastructures, and finally their release to a marketplace.

The main goal of this deliverable is to demonstrate the utilization of validation tools at their final state and the onboarding to the open repository, which were created as part of WP3 and, more specifically, in Task 3.2. These tools are instrumental in overseeing the fully automated validation process using the final prototypes of the Network Applications that have been developed in WP4 and are described in D4.4-D4.7. Additionally, within the same context, the current deliverable provides specific information about the Key Performance Indicators (KPIs) of the Network Application alongside a vertical Application and defends that the integration of the former with the latter yields a satisfactory service delivery. Within the previous deliverable manual validation tests have been conducted on top of use-case driven test-cases/scenarios geared to collect qualitative data/Key Value Indicators (KVIs). Thus, the work outlined in the deliverable paves the way for the subsequent task in WP5, namely T5.4, focusing on the certification process. As soon as the validated Network Applications also pass the certification process, they will be ready to be made publicly available through the EVOLVED-5G Marketplace. This advancement is firmly based on the systematic validation these Network Apps have undergone.

As a final point, in the context of EVOLVED-5G, it is essential to highlight that a terminology update has been implemented. Specifically, the term "Network App" is now being used instead of "NetApp," as initially selected in the first period of the project. This update reflects the shortened form of "Network Application” and has been applied consistently across all project’s documents and materials.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

One of the main objectives of EVOLVED-5G project and WP5 more specifically, is to define and provide validation tests to all the Network Apps. Thus, the current document *"NetApps Validation and onboarding to Open Repository"* provides details on the use of the validation tools and open repository with the aim to validate the Network Apps developed in WP4. Moreover, the document provides details towards the manual validation of a Network App with a vApp, guaranteeing that the coupled Network App-vApp can properly deliver the enhanced features in the provisioned service under different conditions (i.e., the vApp makes proper use of all the capabilities exposed by the Network App).

1.2 STRUCTURE OF THE DOCUMENT

The core part of the document is divided into the following sections:

- **Section 2: Validation Environment** focuses on the Validation Framework that is being utilised for the implementation of the tests that the Network Apps should undergo. This framework includes the Continuous Integration / Continuous Development (CI/CD) tools, the Kubernetes clusters and 5G Network functions that will be installed in the EVOLVED-5G platforms (Athens-Malaga).
- **Section 3: Network Application Key** Performance Indicators is devoted to the Network Applications KPIs both in a horizontal and use case specific point of view.
- **Section 4: Automated Validation Tests** describes the role of the of CI/CD automation server tools and the steps comprising the validation process of the Network Apps.
- **Section 5: Validation Rounds and Overall** results summarizes the reports that have been obtained after using these tools during the validation phase.

1.3 TARGET AUDIENCE

The release of the deliverable is public, intending to expose the overall EVOLVED-5G ecosystem and Network Apps Lifecycle design to a wide variety of research individuals and communities.

From specific to broader, different target audiences for D5.2 are identified as detailed below:

- **Project Consortium:** To validate that all objectives and proposed technological advancements have been analysed and to ensure that, through the proposed Network App's lifecycle phases and the various environments, further work can be concretely derived. Furthermore, the deliverable sets to establish a common understanding among the consortium with regards to:
  - The validation framework used within the EVOLVED-5G platforms for the management and orchestration of the resources and the procedures in the testbeds.
  - The validation process of the Network Apps is realised by the several tools that are geared towards the automation of the process.
- **Industry 4.0 and FoF (Factories of the Future) vertical groups:** To crystallise a common understanding of technologies, and design principles that underline the development of the Network Apps, and to understand the utilisation of the network Application Programmable

Interfaces (APIs) exposed by the 5G Infrastructure. A non-exhaustive list of Industry 4.0-related groups is as follows:

  - Manufacturing industries (including both large and Small Medium Enterprise (SMEs) and IIoT (Industrial Internet of Things) technology providers.
  - European, national, and regional manufacturing initiatives, including funding programs, 5G-related research projects, public bodies and policy makers.
  - Technology transfer organizations and market-uptake experts, researchers, and individuals.
  - Standardisation bodies and Open-Source Communities.
  - Industry 4.0 professionals and researchers with technical knowledge and expertise, who have an industrial professional background and work on industry 4.0-related areas.
  - Industry 4.0 Investors and business angels.

- **Telecom Service Providers:** to engage with verticals and to simplify the way 5G services can be offered to a potential customer or 3rd party service provider.
- **Other vertical industries and group**s**:** To seek impact on other 5G-enabled vertical industries and groups in the long run. Indeed, all the architectural components of the facility are designed to secure interoperability beyond vendor specific implementation and across multiple domains. The same categorization as the above but beyond Industry 4.0 can be of application.
- **The scientific audience, general public and the funding EC Organisation:** To document the work performed and justify the effort reported for the relevant activities. The scientific audience can also get an insight of the validation process of the Network Apps developed by the project.

2 VALIDATION ENVIRONMENT

2.1 VALIDATION ENVIRONMENT REFERENCE ARCHITECTURE

The Validation Framework within the EVOLVED-5G platform serves as a vital tool for efficiently managing and orchestrating resources within the testbed. It maintains its core architecture without significant alterations as presented in Deliverable 5.2 “Network Apps Validation and onboarding to Open Repository”. As it has been described in that deliverable this framework caters to various needs, encompassing both standard validation tests that all Network Apps must undergo throughout their lifecycle and tailored tests sought after by SMEs and vApp developers. These customized tests include tasks like acquiring specific KPIs or verifying particular features.

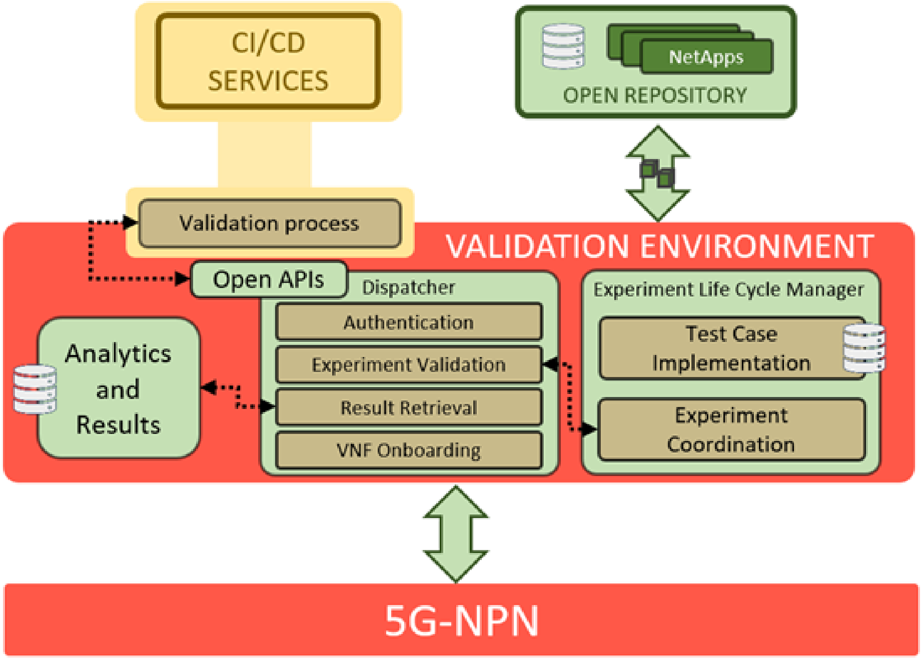


Figure 1 Validation environment reference architecture

The main components of the validation framework have remained consistent with the initial description in Deliverable 5.2 [1] and can be summarized as:

Dispatcher: The front-end of the testbed responsible for authentication, request validation, user management, and resource access. It also supports onboarding Virtual Network Functions (VNFs).

Experiment Life Cycle Manager (ELCM): Manages the execution of experiments, ensuring proper resource usage. It allows for the definition and storage of test cases used in specific experiments that interact with the infrastructure components.

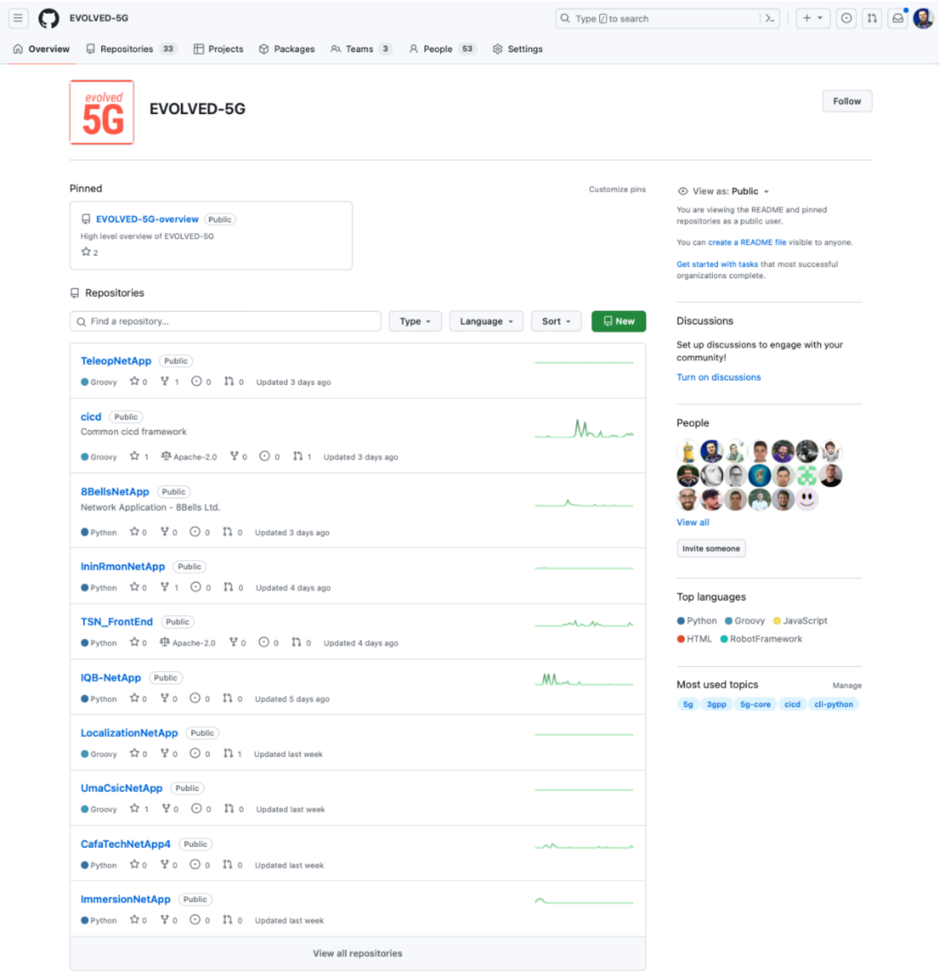
Analytics Module and Results Storage: Provides a long-term solution for storing raw experiment results, along with capabilities for statistical analysis, graphical representation, and in-depth measurement study. These functions are accessible through Open-APIs) implemented by the Dispatcher, consisting of Representational State Transfer (REST) APIs which are utilized by CI/CD services to initiate validation process.

2.2 CI/CD Support For Validation Process

CI/CD Framework was introduced in Deliverable 5.2 and Tools described in D3.2 [2]. The CI/CD tools referred in the previous edition of this deliverable were the Open Repository to store Network Apps images, Jenkins as the Automation orchestration tool, Terraform for Infrastructure as a Code (IaaC) and deployment of Network Apps and robot Framework for test automation. Terraform usage was foreseen as needed to manage Kubernetes clusters and Virtual Machines (VMs) if needed during Network Apps deployments. As all Network Apps have finally opted to use Kubernetes only, the need for using Terraform has diminished. Once the Validation Environment has been setup, we have set up stable Kubernetes clusters both in Málaga and Athens and we have selected Helm as the industry standard to deploy the Network Apps in Kubernetes. Therefore, Terraform tool has been deprecated and replaced by Helm charts.

2.3 Open Repository

Open Repository has not changed since the description that has been provided in D5.2. Github of EVOLVED-5G project (https://github.com/EVOLVED-5G) contains all the Tools and Network Apps validated in EVOLVED-5G, growing up to 30 projects/repositories.



EVOLVED-5G-overview Public
High level overview of EVOLVED-5G
☆ 2

TeleopNetApp Public
Groovy ☆ 0 1 0 0 Updated 3 days ago

cicd Public
Common cicd framework
Groovy ☆ 1 Apache-2.0 0 0 1 Updated 3 days ago

8BellsNetApp Public
Network Application - 8Bells Ltd.
Python ☆ 0 0 0 0 Updated 3 days ago

IninRmonNetApp Public
Python ☆ 0 1 0 0 Updated 4 days ago

TSN_FrontEnd Public
Python ☆ 0 Apache-2.0 0 0 0 Updated 4 days ago

IQB-NetApp Public
Python ☆ 0 0 0 0 Updated 5 days ago

LocalizationNetApp Public
Groovy ☆ 0 0 0 1 Updated last week

UmaCsicNetApp Public
Groovy ☆ 1 0 0 0 Updated last week

CafaTechNetApp4 Public
Python ☆ 0 0 0 0 Updated last week

ImmersionNetApp Public
Python ☆ 0 0 0 0 Updated last week

You are viewing the README and pinned repositories as a public user.

You can create a README file visible to anyone.

Get started with tasks that most successful organizations complete.

Set up discussions to engage with your community!

Turn on discussions

Figure 2 EVOLVED-5G Github repository

2.3.1 Amazon Web Services Elastic Container Registry

Amazon Web Services (AWS) Registry is a private container registry deployed in the public cloud to facilitate the deployment of Network Applications. While the container images are generated in the CI/CD environment at Telefónica´s private network, they need to be accessible for the deployment on Málaga and Athens Kubernetes environments. Therefore, during the Validation process, container images are uploaded to AWS Registry to be grabbed during the deployment steps of the Validation process from Kubernetes clusters at Malaga and Athens. This Registry is also used in Certification process that will be explained thoroughly in D5.6 due at M36.

2.3.2 JFrog Artifactory

JFrog Artifactory has been already described in other deliverables such as D3.4 [3] and D5.2[Missing REF] . It can store all kind of artifacts and it is used during the Validation process to store not only Network Applications artifacts such as container images, but also temporary files produced during the reporting of validation tests, and the validation report produced at the end of the validation process.

2.4 Validation Platforms

To Validate the Network Apps and execute validation tests, whether they are automatic or manual, the Network Apps need to be deployed in containerized infrastructure, namely Kubernetes, and executed in order to test the interaction with Network Exposure Function (NEF) and Common API Framework (CAPIF).

EVOLVED-5G has identified four different container platform instances, each of them with different purposes:

- Three Kubernetes clusters will be associated with the two 5G platforms, Málaga and Athens (NCSRD and COSMOTE clusters). This way, the Network Apps will be deployed in container infrastructure integrated with the 5G platforms.
- The third container infrastructure instance is available in the CI/CD environment. This is independent from 5G platforms and is being used for testing purposes and the integration of EVOLVED-5G Software Development Kit (SDK).

Table 1 Kubernetes Environments usage in Evolved5G

Kubernetes Environment	Verification	Validation	Certification
OpenShift (CI/CD)	✓		
Málaga Kubernetes Cluster		✓	✓
NCSRD Kubernetes Cluster		✓	
COS Kubernetes Cluster			✓

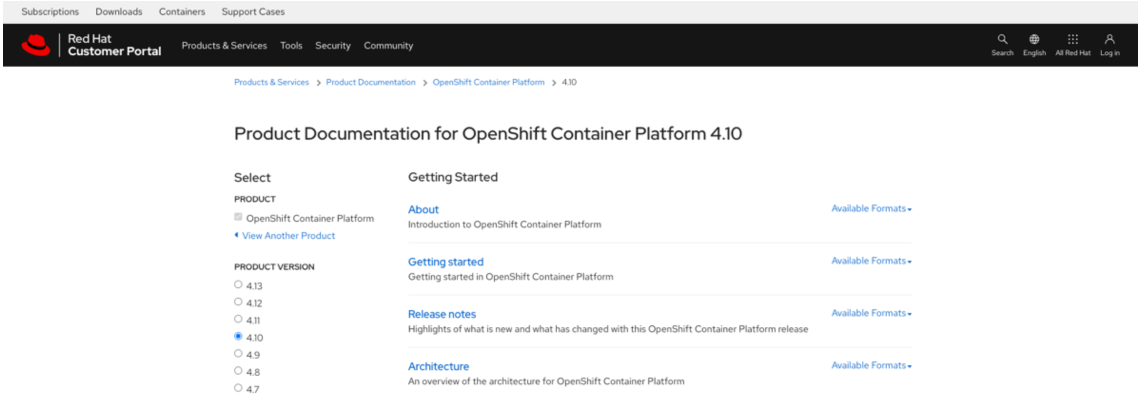
Jenkins pipelines will take as an input parameter the container infrastructure selected to execute the pipeline. For this purpose, Virtual Private Network (VPN) connections have been established between Telefónica´s CI/CD environment and both Málaga and Athens 5G Platforms.

In the following subsections we describe the container platforms infrastructure used in each instance.

2.4.1 OpenShift platform

An initial description of OpenShift Kubernetes platform was provided in D3.2 and D5.2 and extended in D3.4. EVOLVED-5G CI/CD toolset includes a Jenkins slave to interact with OpenShift infrastructure. Thus, Jenkins by using Helm charts can deploy, manage and destroy containers in OpenShift execution platform.

During the project, OpenShift platform has been updated to version 4.10.



Product Documentation for OpenShift Container Platform 4.10

Select

PRODUCT

☑ OpenShift Container Platform

View Another Product

PRODUCT VERSION

○ 4.13
○ 4.12
○ 4.11
● 4.10
○ 4.9
○ 4.8
○ 4.7

Getting Started

About — Introduction to OpenShift Container Platform — Available Formats

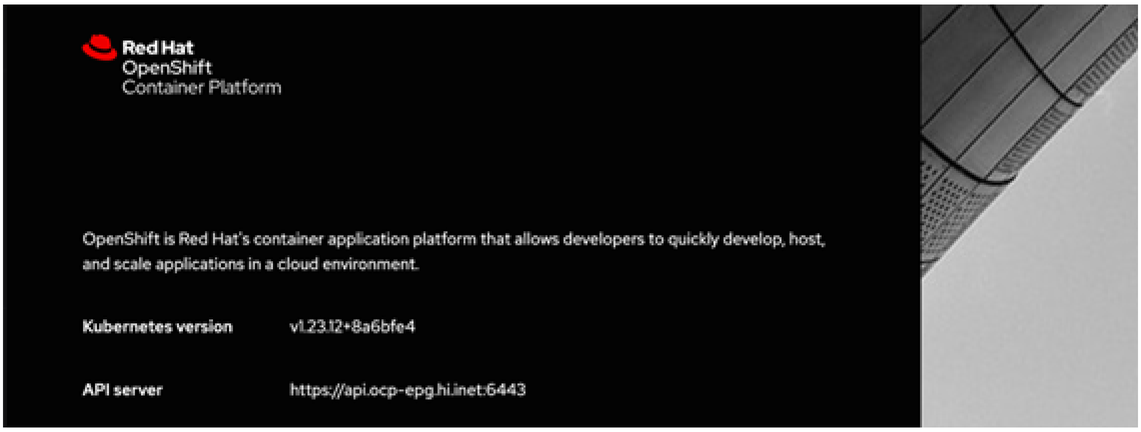
Getting started — Getting started in OpenShift Container Platform — Available Formats

Release notes — Highlights of what is new and what has changed with this OpenShift Container Platform release — Available Formats

Architecture — An overview of the architecture for OpenShift Container Platform — Available Formats

Figure 3 OpenShift version in CICD Environment

This version of OpenShift includes new Kubernetes versions as displayed in the following picture.



OpenShift is Red Hat's container application platform that allows developers to quickly develop, host, and scale applications in a cloud environment.

Kubernetes version v1.23.12+8a6bfe4

API server https://api.ocp-epg.hi.inet:6443

Figure 4 Kubernetes version in CICD Environment

2.4.2 Kubernetes in Athens Platform

2.4.2.1 Kubernetes Athens-NCSRD

The validation tests require the full functionality of a containerized environment provided by the platforms, and consequently the deployment of the Network Apps within this environment. These deployments are essential for testing their interactions with NEF and CAPIF.

The Kubernetes (K8s) cluster used in the Athens Platform consists of three virtual machines (VMs): one master node and two worker nodes. Each of these nodes has the following specifications: 2x vCPUs and 4GB of RAM. Access to these nodes is facilitated through a VPN connection. It's worth noting that the cluster has been updated to use Kubernetes version 1.26.

As part of the final round for the evolution of the platforms described in D3.3 [4] several updates have been made to the cluster to ensure it is ready and functional for the validation phase. Specifically, the Calico networking plugin has been replaced with Cilium. Cilium offers greater flexibility for network connectivity by allowing specific configurations and policies to be defined.

Additionally, NGINX Ingress Controller has been deployed in the cluster. This Ingress Controller follows the NodePort service exposure approach, which means it routes incoming requests to the appropriate service within the cluster. The overall architecture of the Athens K8s cluster on the premises of NCSRD is depicted in Figure 5.

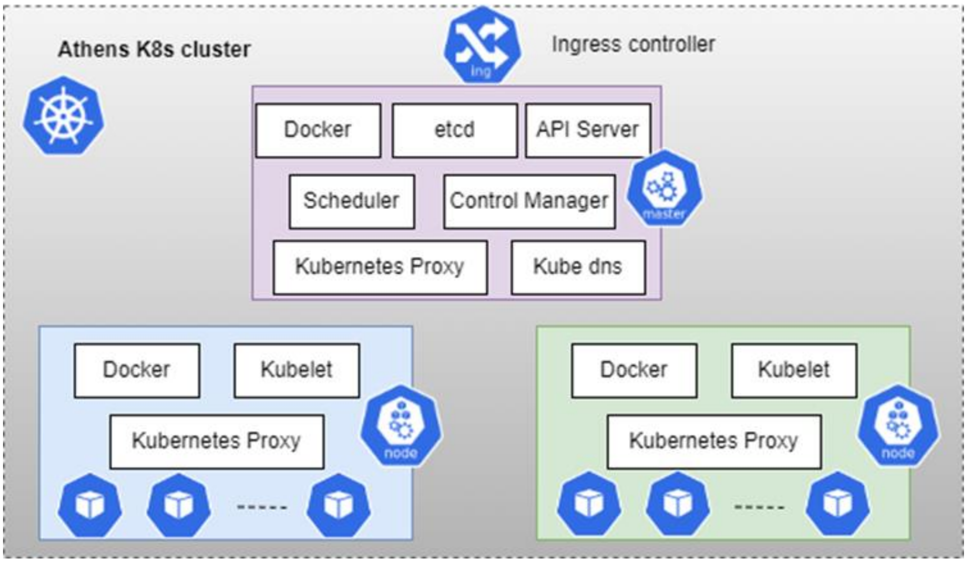


Figure 5 Athens platform K8s (NCSRD site)

2.4.2.2 Kubernetes Athens COSMOTE

COSMOTE Kubernetes cluster has been primarily established an integral part of the Athens certification environment. Its architecture includes a master node overseeing the control plane and two worker nodes executing workloads, running on Kubernetes version 1.25.6. An additional VM functions as a VPN server for secure remote access. The master node has 6 vCPUs, 12 GB of memory, and a 100 GB hard disk. Worker nodes have 16 GB of memory. Calico is the chosen networking plugin for secure pod and service communication. Rancher simplifies cluster setup and management with its user-friendly interface. Docker Engine is used for containerization, ensuring consistent and isolated runtime environments. Prometheus monitors cluster health and performance by collecting crucial metrics, facilitating proactive management and troubleshooting.

The cluster makes use of the Docker Engine as its container runtime, which enables the containerization and efficient management of applications within Docker containers. Docker provides a consistent and isolated runtime environment, which simplifies the packaging, distribution, and deployment of applications. This approach ensures ease of use and portability across different environments. To monitor the cluster's overall health and performance, Prometheus has been chosen as the monitoring solution. Prometheus is responsible for collecting crucial metrics, allowing for in-depth insights into resource utilization, application performance, and the overall health of the cluster. This monitoring capability empowers proactive management and simplifies troubleshooting efforts.

2.4.2.2.1 Integration Activities with GMI on COSMOTE Kubernetes

As described in Deliverable 4.3 (Exposure Capabilities for Vertical Applications) and more specifically in section 5 (Vertical Application and Network Application Integration trials), two rounds of integration activities in the EVOLVED-5G platforms (Athens and Malaga) were performed to demonstrate the functionality of the Network app when seamlessly integrated with the vApp and to test the use case for each Network App overall. During the second round the K8s cluster of each platform served as the testing environment and the outcome successfully showcased the practical benefits of integrating all the components of the EVOLVED-5G ecosystem and validating the various use cases.

Considering the topology of the Athens platform, which spans across two distinct sites - NCSRD and COSMOTE, an additional phase of integration activities was carried out at the COSMOTE premises. During this phase, the Network App developed by GMI, based on the Digital/Physical twin concept under the Interaction of Employees and Machines (IEM), was selected for integration. The integration was performed utilizing COSMOTE's K8s cluster and highlighted the deployment and setup in a different site and environment. Simultaneously, the use case was once again successfully validated, considering various parameters and configurations compared to the integration tests that took place in NCSRD site. To validate this use case at COSMOTE premises, the network setup used was quite similar to the one used for the first round in NCSRD lab, but the aim here was to demonstrate integration with following the latest progress of the project. The various software components were deployed on the Kubernetes cluster this time, with the latest versions of NEF 2.2.2, CAPIF 3.1.2 services and the corresponding network application. The overall architecture and the deployment of the aforementioned services are illustrated in Figure 6 and Figure 7 respectively.

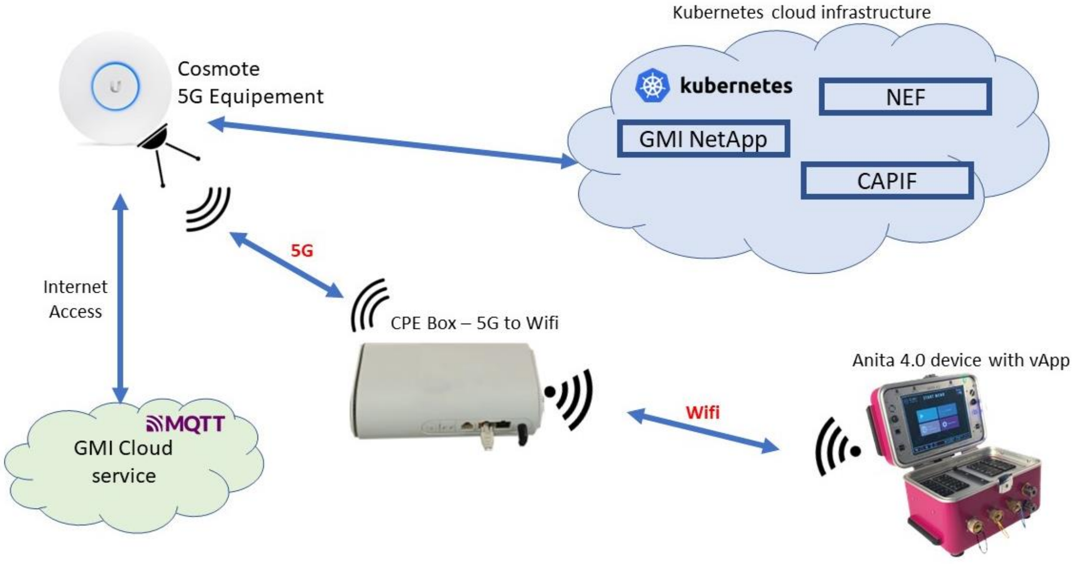
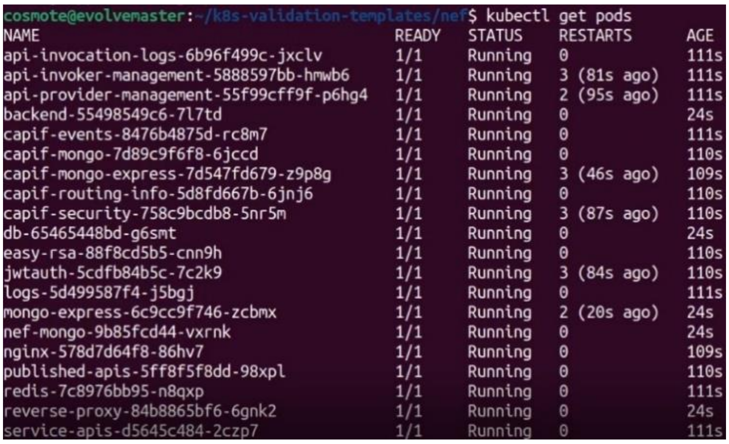


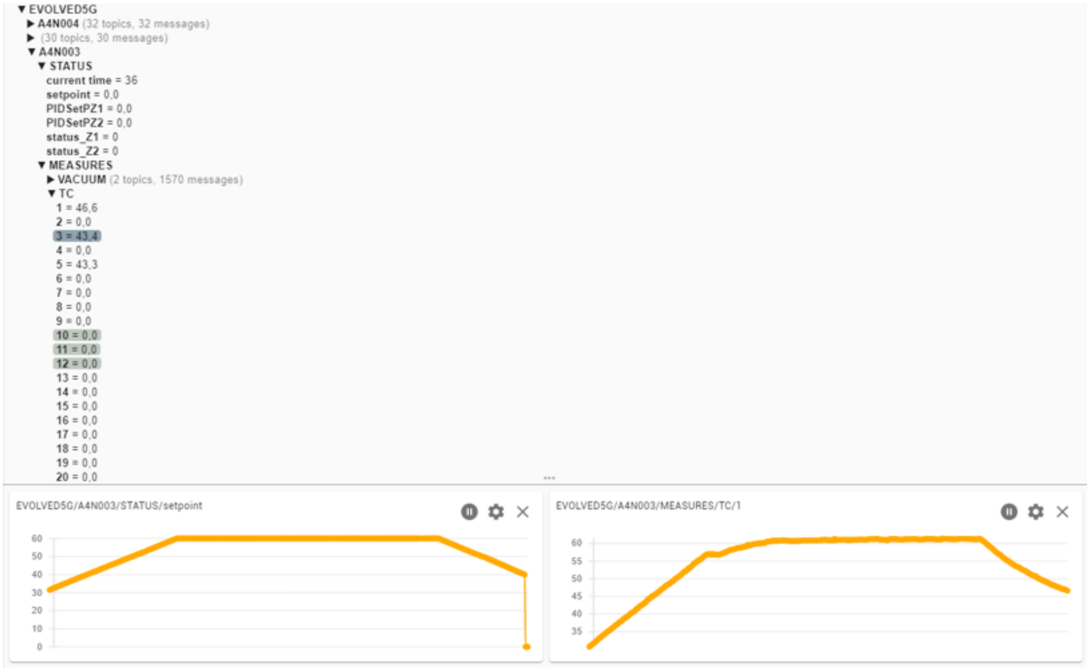
Figure 6 Topology of the testing setup



```
cosmote@evolvemaster:~/k8s-validation-templates/nef$ kubectl get pods
NAME                                      READY   STATUS    RESTARTS      AGE
api-invocation-logs-6b96f499c-jxclv       1/1     Running   0             111s
api-invoker-management-5888597bb-hmwb6    1/1     Running   3 (81s ago)   111s
api-provider-management-55f99cff9f-p6hg4  1/1     Running   2 (95s ago)   111s
backend-55498549c6-7l7td                  1/1     Running   0             24s
capif-events-8476b4875d-rc8m7             1/1     Running   0             111s
capif-mongo-7d89c9f6f8-6jccd              1/1     Running   0             110s
capif-mongo-express-7d547fd679-z9p8g      1/1     Running   3 (46s ago)   109s
capif-routing-info-5d8fd667b-6jnj6        1/1     Running   0             110s
capif-security-758c9bcdb8-5nr5m           1/1     Running   3 (87s ago)   110s
db-65465448bd-g6smt                       1/1     Running   0             24s
easy-rsa-88f8cd5b5-cnn9h                  1/1     Running   0             110s
jwtauth-5cdfb84b5c-7c2k9                  1/1     Running   3 (84s ago)   110s
logs-5d499587f4-j5bgj                     1/1     Running   0             111s
mongo-express-6c9cc9f746-zcbmx            1/1     Running   2 (20s ago)   24s
nef-mongo-9b85fcd44-vxrnk                 1/1     Running   0             24s
nginx-578d7d64f8-86hv7                    1/1     Running   0             109s
published-apis-5ff8f5f8dd-98xpl           1/1     Running   0             110s
redis-7c8976bb95-n8qxp                    1/1     Running   0             111s
reverse-proxy-84b8865bf6-6gnk2            1/1     Running   0             24s
service-apis-d5645c484-2czp7              1/1     Running   0             111s
```

Figure 7 NEF & CAPIF services in Kubernetes

Since the setup and the configurations for NCSR Demokritos and COSMOTE K8s cluster are almost similar, an initial deployment test had been carried out remotely using the Kubernetes platform provided by NCSR Demokritos over the previous days, to check that the Network app was working properly. On the hardware side, the Anita console (see Figure 9) was this time connected by Wi-Fi to another model of CPE device supplied by COSMOTE, which was itself linked to an external 5G access point in standalone configuration. During the validation test, the Anita had to be capable both of communicating with the nginx web server within the Kubernetes containers on the internal network and with the GMI server via external Internet access. Upon the successful setup the data packet transmitted has been appropriately adjusted according to the defined use case Reference to D4.4 [5] and Quality of Service (QoS) requirements. A specialized network tool was employed to visualize the data sent to GMI's cloud server as depicted in Figure 8.



```
▼ EVOLVED5G
  ▶ A4N004 (32 topics, 32 messages)
  ▶ (30 topics, 30 messages)
  ▼ A4N003
    ▼ STATUS
      current time = 36
      setpoint = 0,0
      PIDSetPZ1 = 0,0
      PIDSetPZ2 = 0,0
      status_Z1 = 0
      status_Z2 = 0
    ▼ MEASURES
      ▶ VACUUM (2 topics, 1570 messages)
      ▼ TC
        1 = 46,6
        2 = 0,0
        3 = 43,4
        4 = 0,0
        5 = 43,3
        6 = 0,0
        7 = 0,0
        8 = 0,0
        9 = 0,0
        10 = 0,0
        11 = 0,0
        12 = 0,0
        13 = 0,0
        14 = 0,0
        15 = 0,0
        16 = 0,0
        17 = 0,0
        18 = 0,0
        19 = 0,0
        20 = 0,0
```

EVOLVED5G/A4N003/STATUS/setpoint
60
50
40
30
20
10
0
EVOLVED5G/A4N003/MEASURES/TC/1
60
55
50
45
40
35

Figure 8 Digital twin data on distant server

Figure 9 Anita console deployment

2.4.3 Kubernetes in Malaga Platform

In the Málaga cluster, the nodes are accessed by means of a Load Balancer implemented with MetalLB [6] which allows balancing the traffic load between the services exposed in the different nodes. There is also an Ingress controller implemented with contour that allows a more elaborate way of exposing the services. A role-based policy (RBAC) is used to allow the isolation of users using the cluster. Containerd [7] is used as container runtime, and for networking between the different elements of the system, Calico is used. In addition, KubeVirt [8] is used for the virtualization of VMs in the system over the containerized infrastructure. Finally, for system monitoring, Prometheus is used together with Grafana for the visualization of the measurements taken by the system

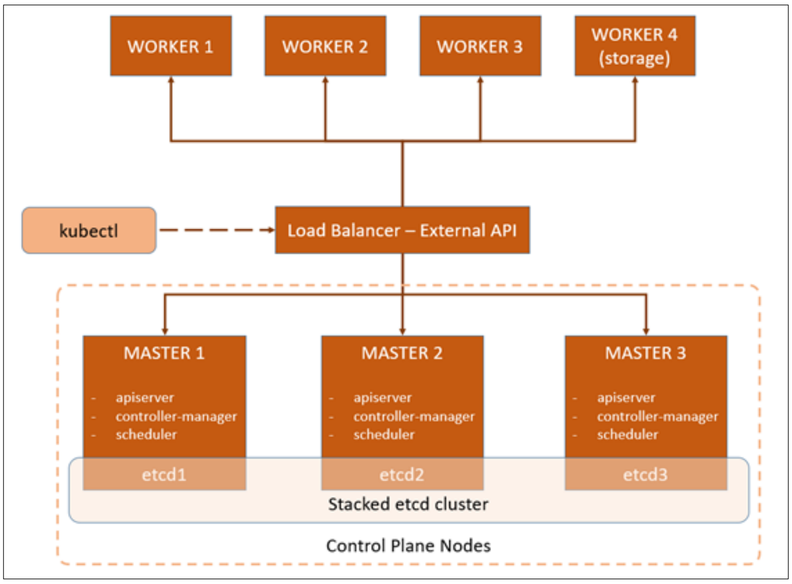


Figure 10 Kubernetes architecture in the Málaga platform

3 Network Application Key Performance Indicators

3.1.1 Horizontal Performance KPIs (Kubernetes cluster)

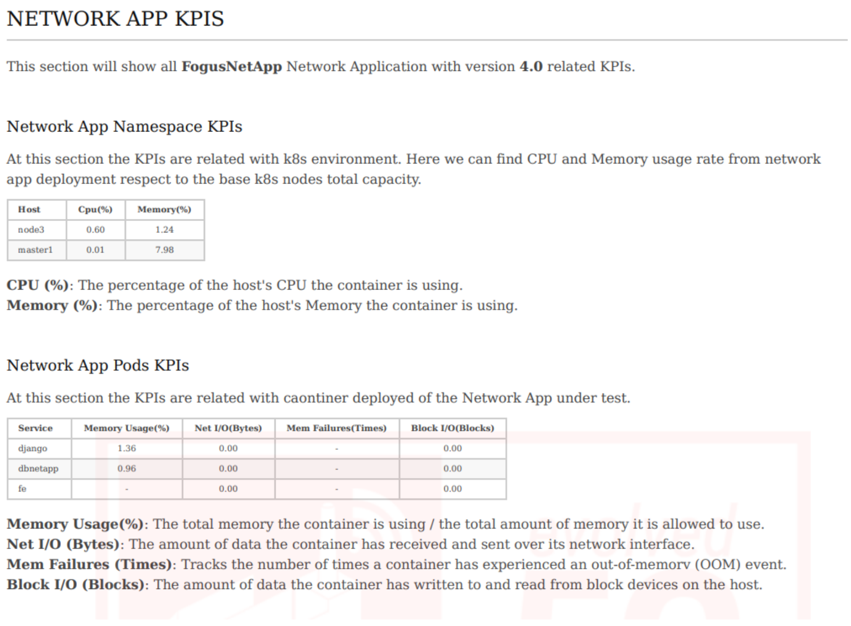
In the framework of Task 5.2 and considering the container-based approach adopted by all Network Applications, we have identified a comprehensive set of universal KPIs. These KPIs, referred to as Docker Container Performance Metrics, have been implemented across all Network Applications, with a specific emphasis on evaluating and optimizing container metrics. The horizontal KPIs can be categorized into two groups: those associated with the Docker hosts and those directly related to the containers.

In order to monitor the docker container Prometheus software has been utilised. The specific tool is an open-source monitoring and alerting system well-suited for monitoring the resource usage and health of Docker containers. For retrieving the metrics for the containers, Prometheus server has been deployed and configured in both the Athens and Malaga environments, ensuring comprehensive monitoring capabilities for the containerized applications. Moreover, the relevant queries have been created to in PromQL language to extract specific metrics related to the Network Apps.

The table below summarizes the specific KPIs that are being targeted along with their definition. It is worth mentioning that the measurement method and the respective measurements are an integral part of the certification process, as it has been incorporated into the certification pipeline and are generated into the final certification report, as can be seen in Figure 11. The breakdown of the certification report that will be presented and described in detail in deliverable D5.6 due at M36 of the project.

Table 2 Docker containers performance stats

KPI	Description
CPU %	The percentage of the host's CPU the container is using
MEM %	The percentage of the host’s Memory the container is using
MEM usage / limit	The total memory the container is using / the total amount of memory it is allowed to use
NET I/O	The amount of data the container has received and sent over its network interface
MEM failures	Tracks the number of times a container has experienced an out-of-memory (OOM) event.
BLOCK I/O	The amount of data the container has written to and read from block devices on the host
Deployment time	How long it takes to deploy a network application in K8s cluster / VMs



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(%)
node3	0.60	1.24
master1	0.01	7.98

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 caontiner deployed of the Network App under test.

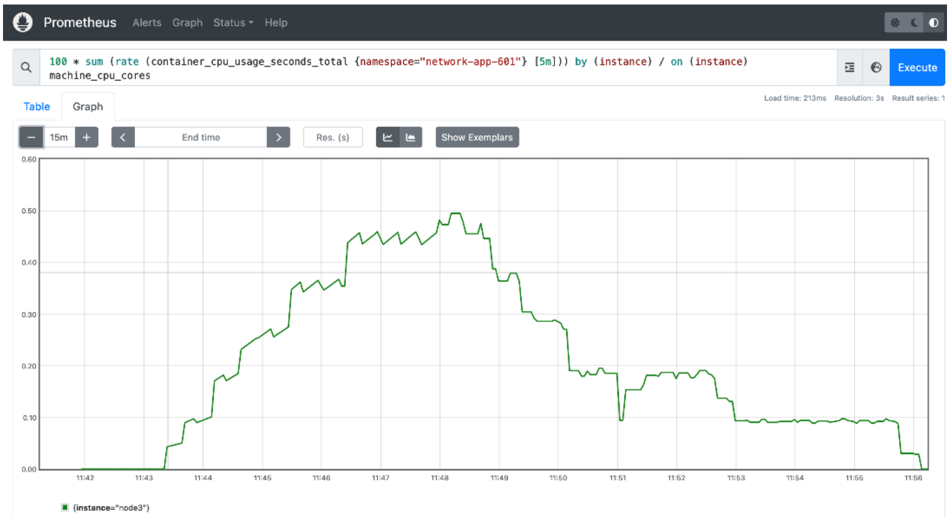
Service	Memory Usage(%)	Net I/O(Bytes)	Mem Failures(Times)	Block I/O(Blocks)
django	1.36	0.00	-	0.00
dbnetapp	0.96	0.00	-	0.00
fe	-	0.00	-	0.00

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-memory (OOM) event.
Block I/O (Blocks): The amount of data the container has written to and read from block devices on the host.

Figure 11 K8s Network Application KPIs as part of the certification report

3.1.1.1 Container CPU usage

One of the most basic bits of information is information about how much processing power of the Central Processor Unit (CPU) is being consumed by all containers, images, or by specific containers. A great advantage of using Docker is the capability to limit CPU utilization by containers. Tuning and optimizing require precise measurements, making monitoring of these limits an indispensable practice. Observing the total duration during which a container's CPU usage experiences throttling furnishes crucial insights for fine-tuning CPU share settings in Docker. It's important to emphasize that CPU time encounters throttling exclusively when the host's CPU utilization reaches its maximum threshold. As long as the host possesses surplus CPU resources available for Docker, containers' CPU usage remains unthrottled. Consequently, the throttled CPU metric typically registers as zero, and any spikes in this metric typically serve as a reliable indicator that one or more containers need greater CPU resources than the host can currently allocate. The figure below illustrates the specific metric retrieved from the Prometheus environment while testing a Network App.



```
100 * sum (rate (container_cpu_usage_seconds_total {namespace="network-app-601"} [5m])) by (instance) / on (instance)
machine_cpu_cores
```

Load time: 213ms Resolution: 3s Result series: 1

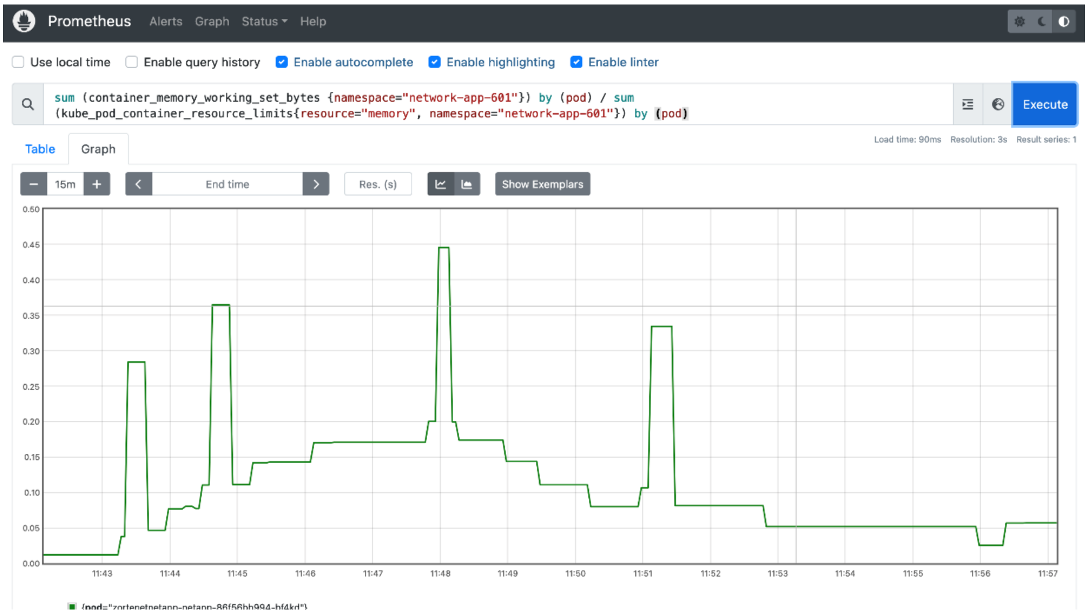
Figure 12 Container CPU usage in Prometheus environment

3.1.1.2 Container Memory usage

Assessing and managing the memory footprint of application containers is a pivotal KPI for maintaining a stable environment. It safeguards optimal application performance while preventing excessive memory usage that could potentially disrupt other containers sharing the same host. Adhering to best practices involves a systematic approach to fine-tuning memory settings, typically conducted in several iterations. The best practice is to tune memory setting in a few iterations:

- Monitor memory usage of the application container
- Set memory limits according to the observations
- Continue monitoring of memory, memory fail counters and Out-Of-Memory (OOM) events.

If OOM events happen, the container memory limits may need to be increased, or debugging is required to find the reason for the high memory consumptions. The following figure is an example of the specific metric retrieved from the Prometheus environment while testing a Network App.



□ Use local time □ Enable query history ☑ Enable autocomplete ☑ Enable highlighting ☑ Enable linter

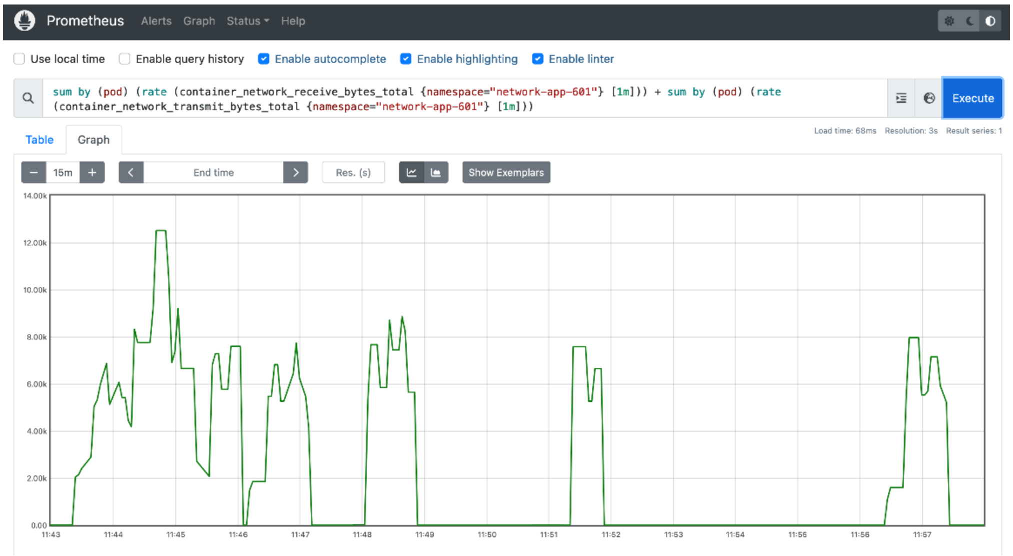
```
sum (container_memory_working_set_bytes {namespace="network-app-601"}) by (pod) / sum
(kube_pod_container_resource_limits{resource="memory", namespace="network-app-601"}) by (pod)
```

Load time: 90ms Resolution: 3s Result series: 1

Figure 13 Container memory usage in Prometheus environment

3.1.1.3 NET I/O

The Network I/O stats show the volume of information the container's network interface has transmitted (TX) and received (RX). It basically represents the traffic of the network. The following figure illustrates the container’s (Network App) received and transmitted bytes, as retrieved from the Prometheus environment.



☐ Use local time ☐ Enable query history ☑ Enable autocomplete ☑ Enable highlighting ☑ Enable linter

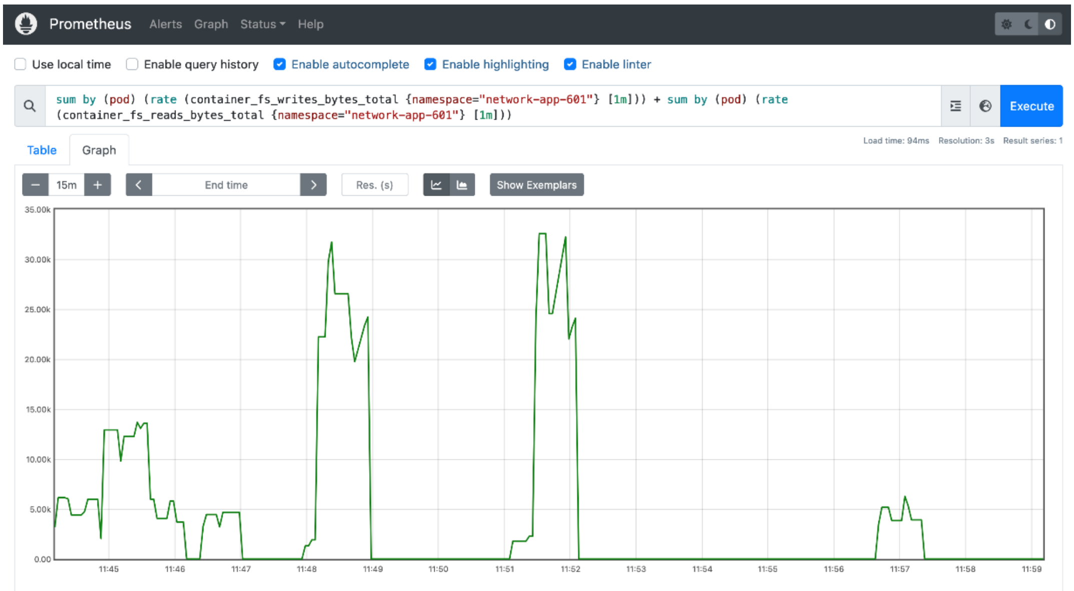
```
sum by (pod) (rate (container_network_receive_bytes_total {namespace="network-app-601"} [1m])) + sum by (pod) (rate
(container_network_transmit_bytes_total {namespace="network-app-601"} [1m]))
```

Load time: 68ms Resolution: 3s Result series: 1

Figure 14 Example of container's network interface Tx and Rx data in Prometheus environment

3.1.1.4 Block I/O

By utilizing the statistics provided by block I/O, containers that are actively reading and writing data to their respective container file systems can be identified. These block I/O statistics offer insights into potential issues related to data persistence. The following figure presents the reading and writing data process of a specific container (Network App) as illustrated in the Prometheus environment.



☐ Use local time ☐ Enable query history ☑ Enable autocomplete ☑ Enable highlighting ☑ Enable linter

```
sum by (pod) (rate (container_fs_writes_bytes_total {namespace="network-app-601"} [1m])) + sum by (pod) (rate
(container_fs_reads_bytes_total {namespace="network-app-601"} [1m]))
```

Load time: 94ms Resolution: 3s Result series: 1

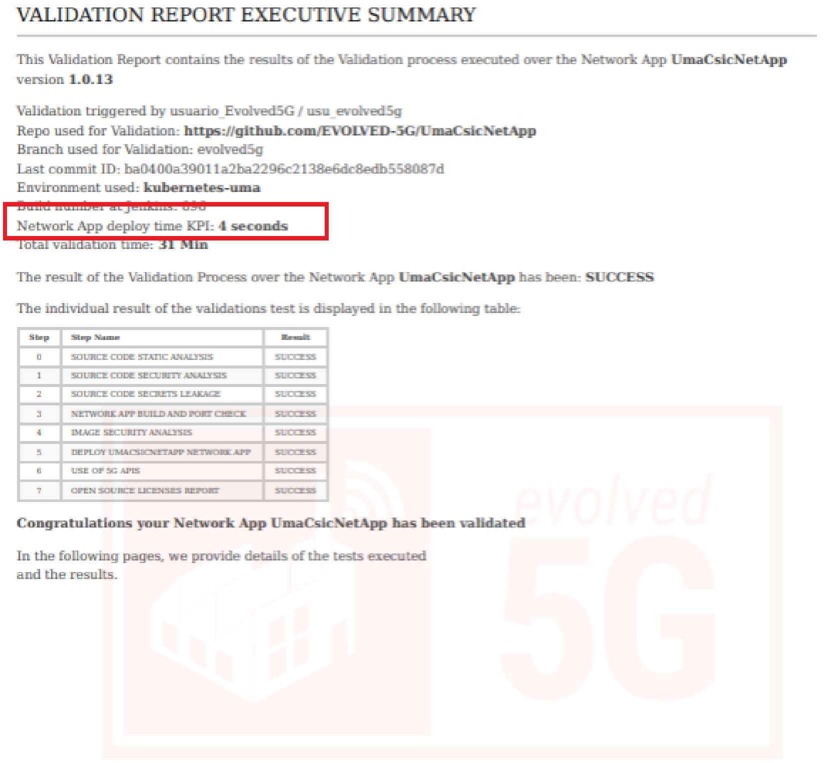
Figure 15 Example of container's reading and writing data process in the Prometheus environment

3.1.1.5 PIDs

PIDs represents the count of processes created within the container or the number of active kernel process IDs running inside that specific container.

3.1.1.6 Network Application Deployment time

The deployment time of a container in Kubernetes (K8s) refers to the duration it takes to set up and make a containerized application operational within a K8s cluster. The deployment time is a crucial performance metric as it reflects the efficiency both on the container orchestration platform (Kubernetes, in this case) and the overall application deployment process. In the light of the above and as part of the validation report, the deployment time of each Network App is being considered as part of the steps performed during the validation pipeline. The deployment time is provided to the Network Apps developers within the final report, as can be seen indicatively for UMA/CSIC Network App for UMA and Athens platform in Figure 12.



VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **UmaCsicNetApp** version **1.0.13**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/UmaCsicNetApp**
Branch used for Validation: evolved5g
Last commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d
Environment used: **kubernetes-uma**
Build number at Jenkins: 696
Network App deploy time KPI: **4 seconds**
Total validation time: **31 Min**

The result of the Validation Process over the Network App **UmaCsicNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App UmaCsicNetApp has been validated

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

Figure 16 Deployment time for Network Application as part of the report

3.1.2 Application level-Business KPIs

In addition to the horizontal approach stemming from the K8s cluster, the project has strategically identified a distinct set of KPIs that reflect the diversity of the Network Apps developed in the context of WP4. These KPIs are tailored to align with the use cases provided in each of the four pillars, adding a layer of granularity to the performance evaluation framework for the Network Apps. Within this context, each SME has contributed a unique set of KPIs, which are primarily driven by their business expectations for their respective product. These KPIs are aimed to demonstrate that the vApp achieves the anticipated performance levels while harnessing the capabilities of the respective Network App defined within their vertical domain.

The anticipated performance levels (from a business perspective) of the Network Apps can be evaluated by comparing them to the performance tests of NEF APIs, as initially provided in Deliverable 5.1, “System-level Evaluation, and KPI Analysis”.

Table 2 presents the results obtained while testing the NEF Emulator. For those tests a threshold value of 500 milliseconds was selected. The tests have been conducted with the rationale to assess the performance of certain features within a given scenario and have been carried out in a way that corresponds to the anticipated outcomes as outlined by the SMEs. In particular, one of the key parameters under examination for the SMEs is the time it takes for the Network App to receive information for a QoS change, as presented in Table 3. This information is conveyed through the NEF response to the Network Apps which must be for example less than 100ms for a group of SMEs (IMM, GMI, CAF, PAL).

So, the timeframe for the Network App to receive notifications of a QoS change is reflected through the NEF test for the QoS subscription update (measured 39,54 ms). The value that has been measured during the NEF test is below the desired value that has been set by the SMEs as a minimum requirement for the vApp to function properly and the overall service to be delivered. Such an example justifies the system's capability to reliably transfer QoS changes to the Network App, meeting both technical requirements and the business objectives outlined by the SMEs.

Table 3 NEF APIs Performance tests

API	Test	Average access time (mS)	Success ratio
Monitoring Events API	List Active Event Subscription	9.046	100% - Success
	Event Subscription Creation	15.463	100% - Success
	Event Subscription Read	9.54	100% - Success
	Event Subscription Update	11.683	100% - Success
	Event Subscription Delete	10.346	100% - Success
AsSession with QoS API	List Active QoS Subscription	36.298	100% - Success
	QoS Subscription Creation	43.313	100% - Success
	QoS Subscription Read	37.885	100% - Success
	QoS Subscription Update	39.954	100% - Success
	QoS Subscription Delete	37.622	100% - Success

Table 4 Business KPIs as defined by the SMEs

	SME	Expected measurements
QoS API	IMM	Time between detection of QoS degradation and vApp notification < 100 ms
		Time for the Network App to be informed about a QoS change (NEF to Network App) < 100 ms
	GMI	Time between detection of QoS degradation and notification to Anita device < 100ms
	CAF	Time from QoS detection to vApp behavior change<100 ms
	PAL	Each topic to be passed through NEF should be providing a good user experience<100 ms

Combining the information of the abovementioned tables, the following chart in Figure 17 can be extracted. In this chart, the primary vertical axis on the left is used for the Average access time (ms) of the NEF tests, whereas the secondary vertical axis on the right side is for the threshold (ms), as defined from the SMEs in Table 3 for the expected/desirable measurements of the QoS API. As it can be observed, each measurement coming from the NEF tests is consistently below the defined threshold defined by the "business" KPIs of the SMEs in Table 3. Operating consistently below the threshold reflects the efficiency and reliability of the Network App ensures a seamless user experience for each of the use cases that correspond to the Network Apps.

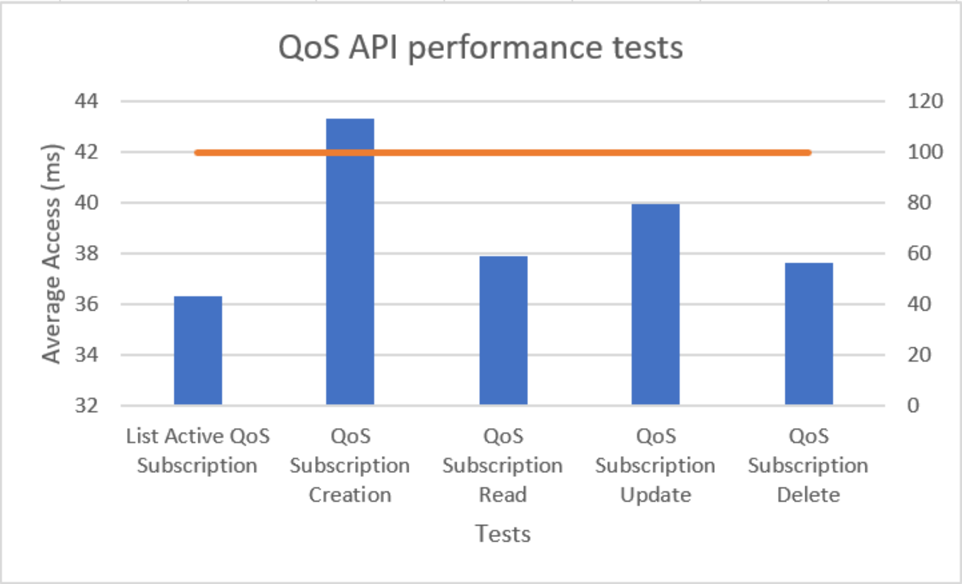


Figure 17 QoS NEF performance tests vs threshold defined by SMEs scenarios

By exploring the information from Table 2 we can create a chart that illustrates the relationship between the Average access time (measured in milliseconds) for the NEF tests related to the Monitoring event on the primary vertical axis, to the threshold (measured in milliseconds) defined by two SMEs that are utilising this API on the secondary vertical axis on the right side.

Table 5 Business KPIs stemming from the SMEs using the Monitoring event API

	SME	Expected measurements per
Monitoring Event API	FOG	Time between NEF Monitoring notification and appearance of UE in vApp (SIEM) < 150 ms
	UMS	If the UE changes from Cell ID1 to CellID2, The Network App should update the output number on the cell ID ROS topic <150 ms

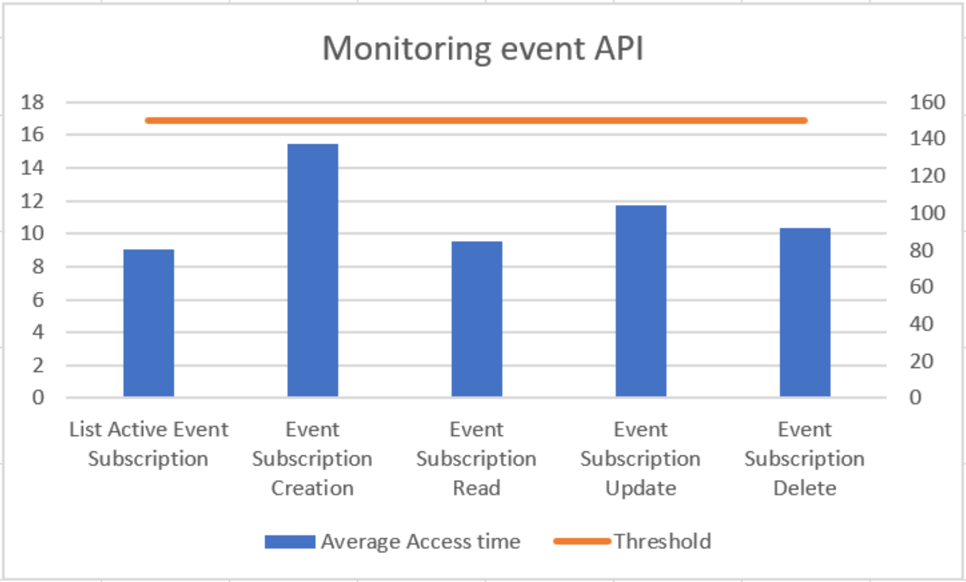


Figure 18 Monitoring event API NEF performance tests vs threshold defined by specific scenarios

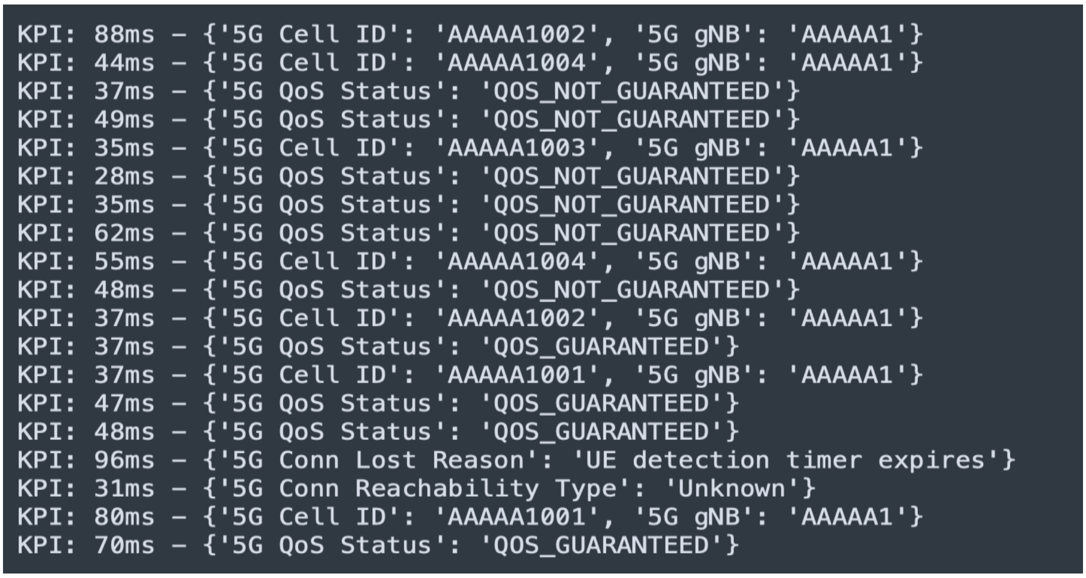
The aforementioned benchmarking process serves as a valuable reference point, enabling the assessment of how the Network apps perform against established benchmarks, namely NEF performance tests. In addition to the theoretical definition of the desired/expected measurements by the SMEs, there are also cases where monitoring and measurement capabilities have been integrated and measured directly within the Network App.

For example, in the case of Industrial Grade 5G Connectivity Network App these internal KPIs are specifically designed to assess the performance of the Network App against predefined criteria utilising the two APIs (AsSessionwithQoS, Monitoring) and the specific events (Location monitoring, Loss of connectivity, UE reachability). In the following table the example of the Industrial Grade 5G Connectivity Network App is presented. Subsequently Figure 19 illustrates the measurements for the specific events as obtained from the Network App.

Table 6 KPIs for Network App -vertical App (Industrial Grade 5G) interaction with NEF APIs

API/Event	Test	Description	Theoretical/expected KPI	Measured KPI
NEF – Location-monitoring	NetworkApp -Location Monitoring event test	When UE (e.g., IoT GW) change location event is received, i.e., Cell ID, vertical App is notified (IoT Management)	1000 ms	~90 ms

NEF-QoS monitoring	Network App - QoS Session event test	When 5G Network QoS event is received (e.g., QOS_GURANTEED, QOS_NOT_GUARANTEED), Vertical App is notified (IoT Management)	1000 ms	~70 ms
	Network App -QoS Session action test	When 5G Network QoS event is received (e.g., QOS_GURANTEED, QOS_NOT_GUARANTEED), Vertical App (IoT GW) takes appropriate action (e.g., enables/disables video stream)	1000 ms	~70 ms
Monitoring Event API-Loss of Connectivity	Network App-Connectivity Loss event test	When Connectivity Loss event is received, vertical App is notified (IoT Management)	1000ms	~ 100ms
Monitoring Event API-UE Reachability	Network App UE Reachability event test	When UE Reachability event is received, vertical App is notified (IoT Management)	1000ms	~ 50ms



```
KPI: 88ms - {'5G Cell ID': 'AAAAA1002', '5G gNB': 'AAAAA1'}
KPI: 44ms - {'5G Cell ID': 'AAAAA1004', '5G gNB': 'AAAAA1'}
KPI: 37ms - {'5G QoS Status': 'QOS_NOT_GUARANTEED'}
KPI: 49ms - {'5G QoS Status': 'QOS_NOT_GUARANTEED'}
KPI: 35ms - {'5G Cell ID': 'AAAAA1003', '5G gNB': 'AAAAA1'}
KPI: 28ms - {'5G QoS Status': 'QOS_NOT_GUARANTEED'}
KPI: 35ms - {'5G QoS Status': 'QOS_NOT_GUARANTEED'}
KPI: 62ms - {'5G QoS Status': 'QOS_NOT_GUARANTEED'}
KPI: 55ms - {'5G Cell ID': 'AAAAA1004', '5G gNB': 'AAAAA1'}
KPI: 48ms - {'5G QoS Status': 'QOS_NOT_GUARANTEED'}
KPI: 37ms - {'5G Cell ID': 'AAAAA1002', '5G gNB': 'AAAAA1'}
KPI: 37ms - {'5G QoS Status': 'QOS_GUARANTEED'}
KPI: 37ms - {'5G Cell ID': 'AAAAA1001', '5G gNB': 'AAAAA1'}
KPI: 47ms - {'5G QoS Status': 'QOS_GUARANTEED'}
KPI: 48ms - {'5G QoS Status': 'QOS_GUARANTEED'}
KPI: 96ms - {'5G Conn Lost Reason': 'UE detection timer expires'}
KPI: 31ms - {'5G Conn Reachability Type': 'Unknown'}
KPI: 80ms - {'5G Cell ID': 'AAAAA1001', '5G gNB': 'AAAAA1'}
KPI: 70ms - {'5G QoS Status': 'QOS_GUARANTEED'}
```

Figure 19 KPIs measurements for QoS and Monitoring API for Industrial grade 5G Connectivity Network App

In this approach, a mapping is presented for each expected measurement/behavior associated with each network application for a given use case. This mapping includes a corresponding description and the means of achieving it

Table 7 Cumulative KPIs and means of achievement

SME	**Related API/Manual Test**	**Description of the desired KPI**	**Pass/Fail**	**Means of achievement/Reference**
IMM	QoS API	Time between detection of QoS degradation and end-users' notification (technician and remote experts notified on the vApp side) < 1s	✓	NEF performance tests as presented in Table 2
		Time between detection of QoS degradation and vApp service adaptation < 10s in case of minor QoS issue	✓	NEF performance tests as presented in Table 2
		Time between detection of QoS degradation and vApp service adaptation < 5s in case of significant QoS issue	✓	NEF performance tests as presented in Table 2
		Time between detection of QoS degradation and vApp service adaptation < 1s in case of critical QoS issue (ex: network failure)	✓	NEF performance tests as presented in Table 2
GMI	Monitoring Event API	Time between detection of QoS degradation and notification to Anitas < 10-15s	✓	NEF performance tests as presented in Table 2
		Able to track the location of UEs with an accuracy of *10*	✓	NEF emulator functional tests presented in Del 5.4
INF	Monitoring Event API	Able to track the location of *50 UEs* simultaneously	✓	NEF emulator functional tests presented in Del 5.4
		Able to track the location of 50 UEs with an accuracy of 1m	✓	- NEF emulator functional tests presented in Del 5.4 - Companion app functionality which provides the location of the UEs Del 3.3 section 6.1.5.1
FOG	Monitoring Event API	Time between NEF monitoring notification and	✓	NEF performance tests as presented in Table 2

		appearance of UE in vApp < 300 ms		
		Percentage of successfully captured real events/data produced by NEF	✓	Manual validation tests described in Del 5.2 section 3
ININ	Monitoring event API	When UE (e.g., IoT GW) change location event is received, i.e., Cell ID, vertical App is notified (IoT Management) <1000 ms	✓	Monitoring Event API - NEF performance tests as presented in Table 2
	QoS API	When 5G Network QoS event is received (e.g., QOS_GURANTEED, QOS_NOT_GUARANTEED), Vertical App is notified (IoT Management) <1000 ms	✓	QoS API -NEF performance tests as presented in Table 2
	QoS API	When 5G Network QoS event is received (e.g., QOS_GURANTEED, QOS_NOT_GUARANTEED), Vertical App (IoT GW) takes appropriate action (e.g., enables/disables video stream) <1000 ms	✓	QoS API -NEF performance tests as presented in Table 2
	Monitoring event API	When Connectivity Loss event is received, vertical App is notified (IoT Management) <1000 ms	✓	Monitoring Event API NEF performance tests as presented in Table 2
	Monitoring event API	When UE Reachability event is received, vertical App is notified (IoT Management) <1000 ms	✓	Monitoring Event API NEF performance tests as presented in Table 2
8Bells	QoS API	Time between detection of QoS degradation (congestion) and throttling applies (vApp) <100 ms	✓	QoS API -NEF performance tests in Table 2
PAL-UMS	Monitoring event API	When the UE changes cellID, the NetworkApp is notified < 100 ms	✓	Monitoring Events API - NEF performance tests in Table 2
IQB	Monitoring Event API	When the UE changes cellID, the callback server is notified < 100 ms	✓	Monitoring Events API - NEF performance tests in Table 2
	Subscription test	Location monitotring subscription for UE	✓	Manual validation tests described in Del 5.2 section 3
	Update subscription test	Updating the subscription of a specific UE	✓	Manual validation tests described in Del 5.2 section 3
	Unsubscribe test	A subscription for a specific UE can be removed	✓	Manual validation tests described in Del 5.2 section 3

	Login test	Login through Keycloak	✓	Manual validation tests described in Del 5.2 section 3
	Unauthorised user test	Unauthorised user is not allowed to use the endpoints	✓	Manual validation tests described in Del 5.2 section 3
CAF	QoS API	NetworkApp notifies vApp about received QoS change	✓	Manual validation tests described in Del 5.2 section 3
ZORT		NetworkApp notifies vApp (dashboard) about received QoS and the operation is halted	✓	Manual validation tests described in Del 5.2 section 3
PAL	User Experience	Each ROS topic that is passed through the 5G should be providing a good user experience	✓	Manual validation tests described in Del 5.2 section 3
	Frequency of topics	The frequency of the topics should be stable	✓	Manual validation tests described in Del 5.2 section 3

4 Automated Validation Tests -final

The Validation Process as defined in EVOLVED-5G includes specific automated steps in order to be considered completed. The Validation steps are thoroughly described in section 4.2. The idea behind the Automated Validation Process is to build the Network Application in a "clean" environment that contains the infrastructure and tools needed to perform all the testing to the Network Application and generate a Validation Report for the Network Application developers with the results. This automated process can be repeated as many times as needed by the Network application developers until they complete their Network Apps development.

This Validation phase has been defined in EVOLVED-5G methodology as a prerequisite for Network Applications to face the Certification Process. By fulfilling all Validation Tests, developers have the certainty that functional requirements regarding the interaction between the Network Application and the 5G infrastructure are met so the confidence to complete the Certification Process increases significantly. Typically, Certification Processes have a cost for the developers and Validation helps developers to get there. The automated validation tests have been defined with scope to assess the Network Applications proper deployment as well as its correct interaction with other 5G network components such as CAPIF, NEF and Time Sensitive Networking (TSN). Those tools are also described in detail in the following sections.

4.1 Tools For Automation

This subsection focuses on the characteristics and role of the of CI/CD automation server tools, as part of the automated validation tests (namely Jenkins, Helm and RobotFramework). Jenkins is used to automate every process in EVOLVED-5G, following one-click automation best practices, RobotFramework [9] is utilised to validate the proper performance of CAPIF and NEF, as well as their integration with Network Apps and Helm charts will be used to deploy Network Applications in the Kubernetes Infrastructure to perform the automated tests.

4.1.1 Jenkins

As described in Deliverable 3.2 [2] and extended in D3.4 [3], Jenkins is an industry-leading open-source automation server in charge of orchestrating a chain of actions related to building, deploying and testing software. In this section there is a focus on the role of Jenkins in the validation phase. To automate the validation process within the lifecycle of the Network Apps, EVOLVED-5G within the overall architecture, has defined a validation pipeline (further description can be found in section 4.3.1, where all validation steps are thoroughly depicted).

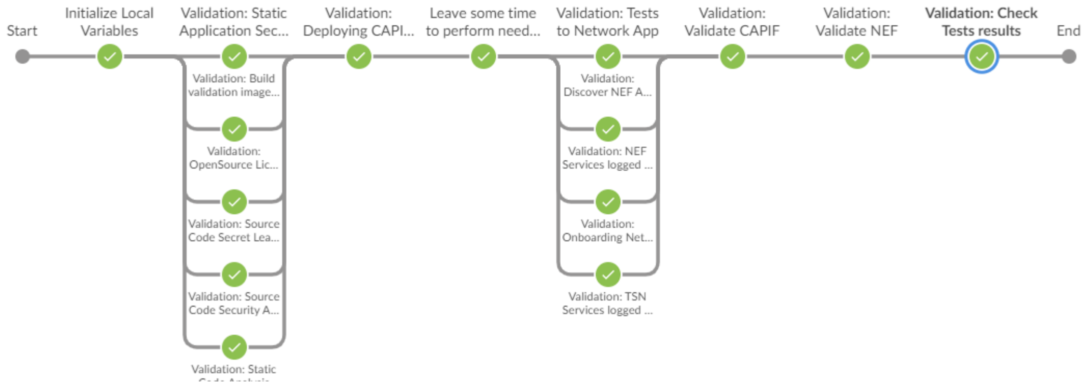
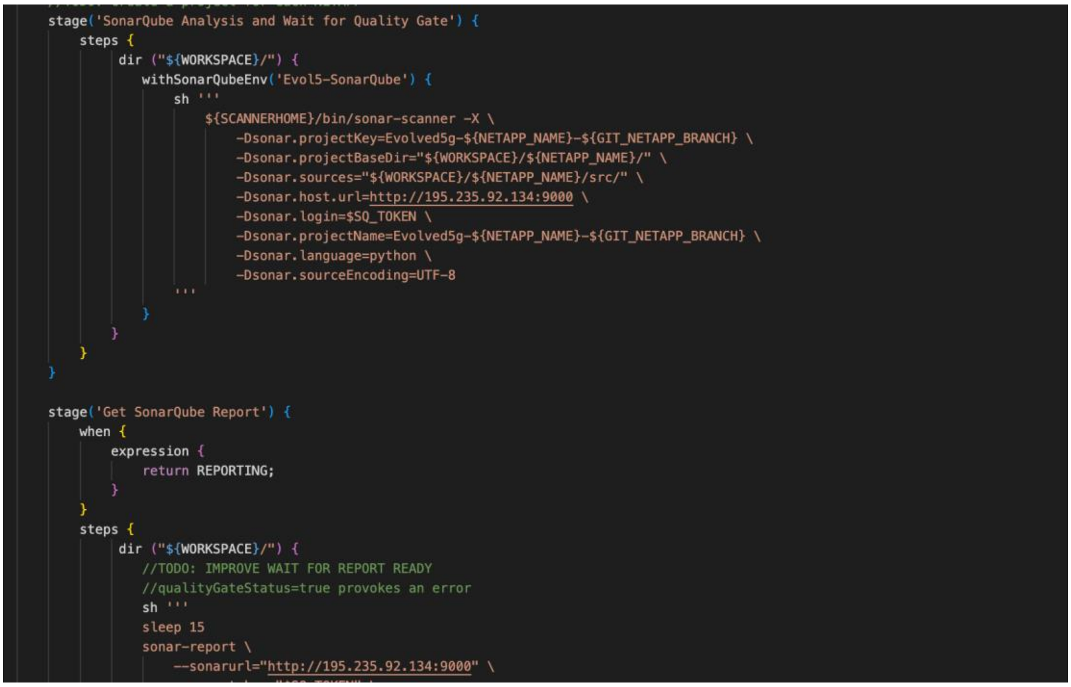

Start
Initialize Local Variables
Validation: Static Application Sec...
Validation: Deploying CAPI...
Leave some time to perform need...
Validation: Tests to Network App
Validation: Validate CAPIF
Validation: Validate NEF
Validation: Check Tests results
End
Validation: Build validation image...
Validation: OpenSource Lic...
Validation: Source Code Secret Lea...
Validation: Source Code Security A...
Validation: Static
Validation: Discover NEF A...
Validation: NEF Services logged ...
Validation: Onboarding Net...
Validation: TSN Services logged ...

Figure 20 Jenkins pipeline flow

In Figure 20 all the steps that are defined in the validation process (i.e., validation steps) are executed by a specific slice of the pipeline, called “stage”. In each of these steps, Jenkins will be the orchestrator for executing commands wrote in each of them. Figure 21 illustrates an example of the definition of a stage in a pipeline, where the execution of specific commands is automatically performed, aiming to generate a Sonarqube [10] report to a specific GitHub Repository.



```
stage('SonarQube Analysis and Wait for Quality Gate') {
    steps {
        dir ("${WORKSPACE}/") {
            withSonarQubeEnv('Evol5-SonarQube') {
                sh '''
                    ${SCANNERHOME}/bin/sonar-scanner -X \
                        -Dsonar.projectKey=Evolved5g-${NETAPP_NAME}-${GIT_NETAPP_BRANCH} \
                        -Dsonar.projectBaseDir="${WORKSPACE}/${NETAPP_NAME}/" \
                        -Dsonar.sources="${WORKSPACE}/${NETAPP_NAME}/src/" \
                        -Dsonar.host.url=http://195.235.92.134:9000 \
                        -Dsonar.login=$SQ_TOKEN \
                        -Dsonar.projectName=Evolved5g-${NETAPP_NAME}-${GIT_NETAPP_BRANCH} \
                        -Dsonar.language=python \
                        -Dsonar.sourceEncoding=UTF-8
                '''
            }
        }
    }
}

stage('Get SonarQube Report') {
    when {
        expression {
            return REPORTING;
        }
    }
    steps {
        dir ("${WORKSPACE}/") {
            //TODO: IMPROVE WAIT FOR REPORT READY
            //qualityGateStatus=true provokes an error
            sh '''
            sleep 15
            sonar-report \
                --sonarurl="http://195.235.92.134:9000" \
```

Figure 21 Jenkins’s pipeline definition.

4.1.2 Robot Framework

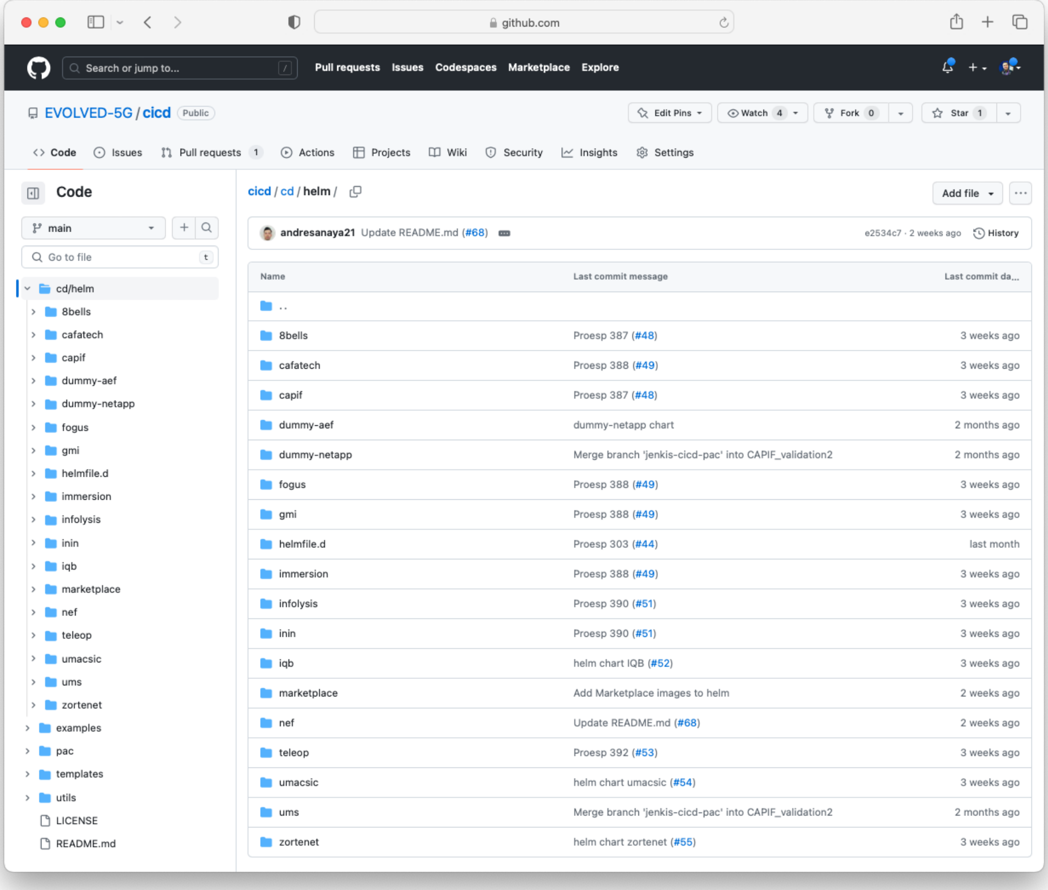
As described in Deliverable 3.2 [2] and extended in D3.4 [3], Robot Framework [11] is the tool used for automated testing purposes in EVOLVED-5G. In the validation process, RobotFramework will automatically test the deployment and configuration of the CAPIF, NEF Emulator and TSN Application Function. For this purpose, several test suites have been developed, following as a reference the 3GPP TS 23.222 [12], 3GPP TS 29.522 [13] 3GPP TS 33.122 [14]and TS 29.122 [15] specifications.

4.1.3 Helm Charts

Initially, Terraform tool was initially selected to manage Infrastructure as Code and create the Kubernetes infrastructure to deploy the Network Applications in those clusters. However, Kubernetes environments that were created do not require dynamic creation and destruction of Kubernetes cluster. Instead, stable Kubernetes clusters are used for this purpose.

Therefore, we have selected Helm [16] to deploy Network Applications in Kubernetes environments. Indeed, Helm is a popular open-source tool designed to simplify the deployment and management of applications within Kubernetes clusters and has been described in D3.4 [3].

Helm chart files for Network Applications and auxiliary tools in EVOLVED-5G are located at https://github.com/EVOLVED-5G/cicd/tree/main/cd/helm



andresanaya21 Update README.md (#68) e2534c7 · 2 weeks ago

Name	Last commit message	Last commit da...
..		
8bells	Proesp 387 (#48)	3 weeks ago
cafatech	Proesp 388 (#49)	3 weeks ago
capif	Proesp 387 (#48)	3 weeks ago
dummy-aef	dummy-netapp chart	2 months ago
dummy-netapp	Merge branch 'jenkis-cicd-pac' into CAPIF_validation2	2 months ago
fogus	Proesp 388 (#49)	3 weeks ago
gmi	Proesp 388 (#49)	3 weeks ago
helmfile.d	Proesp 303 (#44)	last month
immersion	Proesp 388 (#49)	3 weeks ago
infolysis	Proesp 390 (#51)	3 weeks ago
inin	Proesp 390 (#51)	3 weeks ago
iqb	helm chart IQB (#52)	3 weeks ago
marketplace	Add Marketplace images to helm	2 weeks ago
nef	Update README.md (#68)	2 weeks ago
teleop	Proesp 392 (#53)	3 weeks ago
umacsic	helm chart umacsic (#54)	3 weeks ago
ums	Merge branch 'jenkis-cicd-pac' into CAPIF_validation2	2 months ago
zortenet	helm chart zortenet (#55)	3 weeks ago

Figure 22 Helm chart files used by Validation Process

4.2 VALIDATION PIPELINE –UPDATES AND ENHANCEMENTS

An initial description of the Validation Pipeline was provided in D5.2. After the implementation has been completed this is the final list of steps implemented in the Validation Pipeline that orchestrate the automated Validation process, displayed in Figure 23. There are significant changes in the names and order in the final implementation derived from the naming of the tools used to implement some of the steps and the dependencies between different steps.

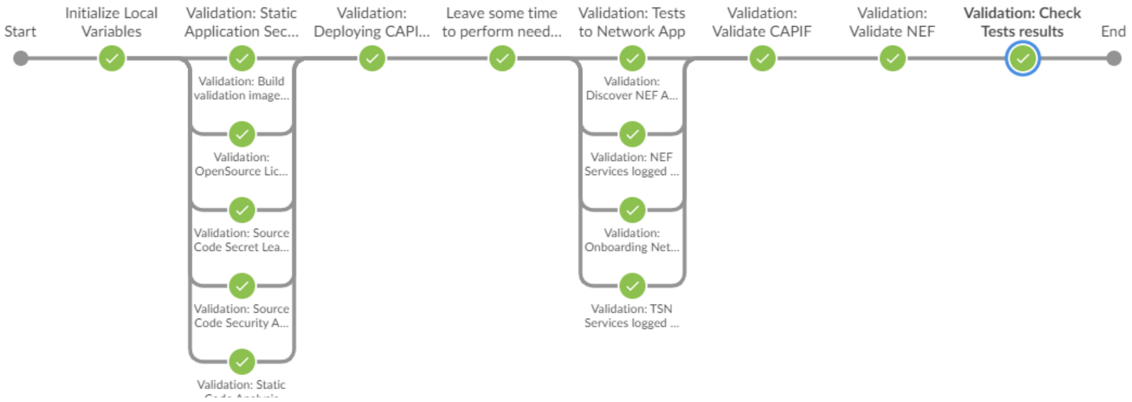
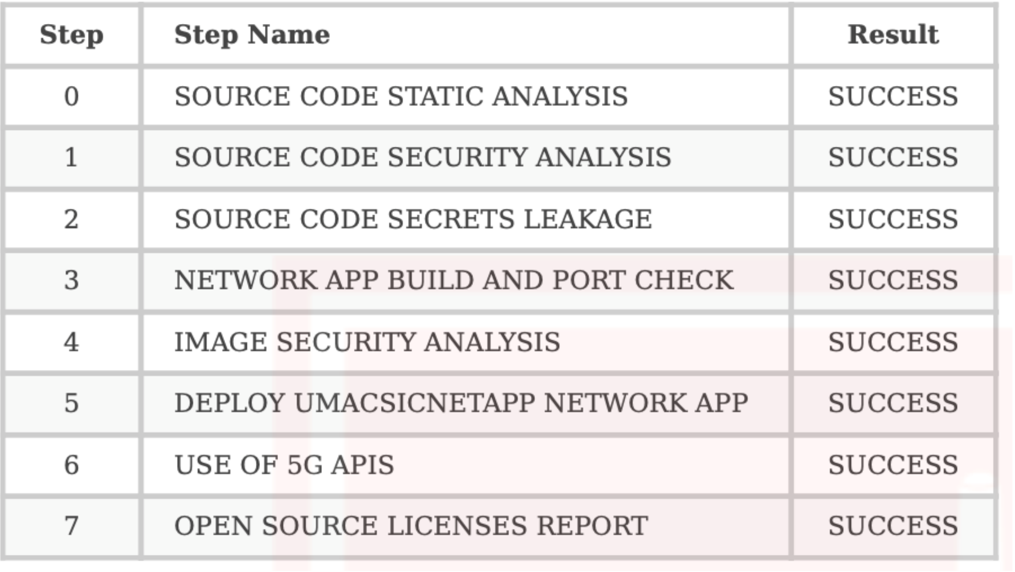

Start
Initialize Local Variables
Validation: Static Application Sec...
Validation: Deploying CAPI...
Leave some time to perform need...
Validation: Tests to Network App
Validation: Validate CAPIF
Validation: Validate NEF
Validation: Check Tests results
End
Validation: Build validation image...
Validation: OpenSource Lic...
Validation: Source Code Secret Lea...
Validation: Source Code Security A...
Validation: Static
Validation: Discover NEF A...
Validation: NEF Services logged ...
Validation: Onboarding Net...
Validation: TSN Services logged ...

Figure 23 Jenkins Validation pipeline

4.2.1 Validation Steps

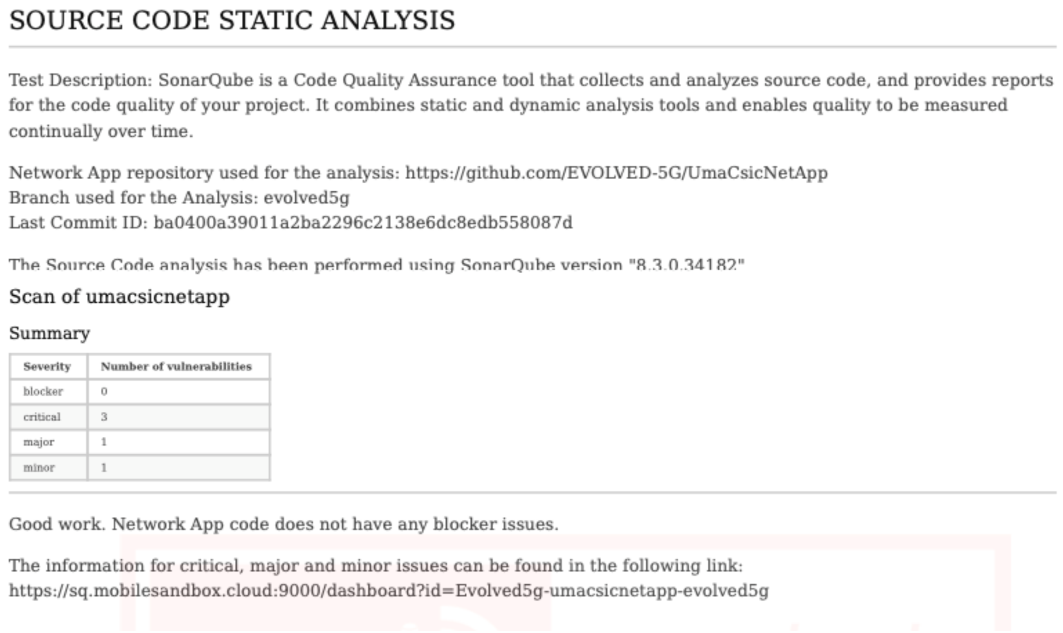
The Validation Pipeline has been structure in EIGHT steps that are reported in the Validation report Summary page as follows:



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

Figure 24 Summary report of Validation Steps

Step 0 – Source Code Static Analysis: This step will obtain some quality code metrics in order to ensure good quality in the developed code. For this operation, Jenkins will use SonarQube version "8.3.0.34182". The results of this step are displayed in the Static Code Analysis Results page in the Validation Report:



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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

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

Scan of umacsicnetapp

Summary

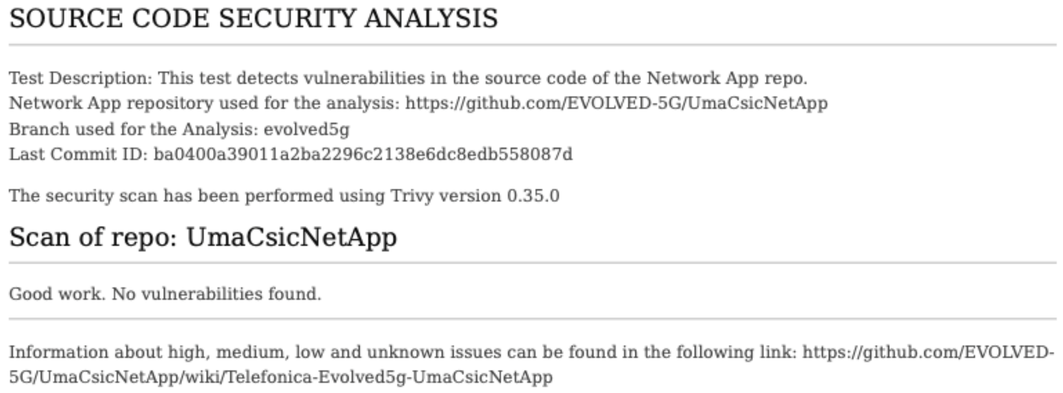
Severity	Number of vulnerabilities
blocker	0
critical	3
major	1
minor	1

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-umacsicnetapp-evolved5g

Figure 25 Source Code Static Analysis Report Page

Step 1 – Source Code Security Analysis: This step will scan the Source Code to find vulnerabilities. For this operation, Jenkins will use Trivy Compliance external tool [15] version 0.35.



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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

The security scan has been performed using Trivy version 0.35.0

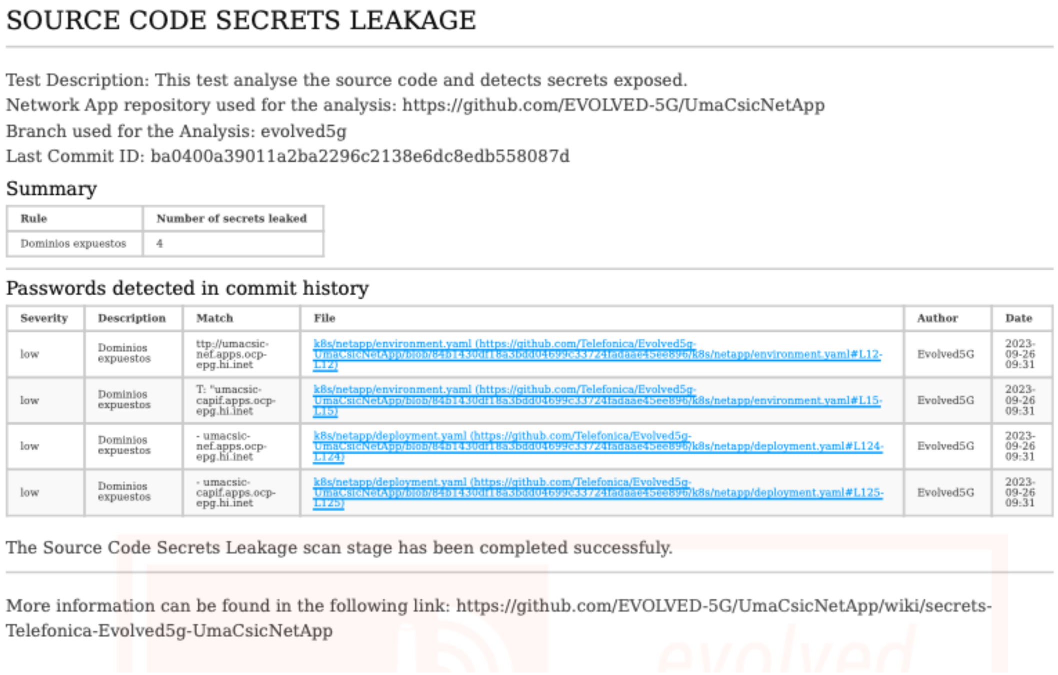
Scan of repo: UmaCsicNetApp

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/UmaCsicNetApp/wiki/Telefonica-Evolved5g-UmaCsicNetApp

Figure 26 Source Code Security Analysis Report Page

Step 2 - Source Code Secret leakage: This step will check if there has been any secret leakage in the git history of the Network App repository. Trivy will be used for this step as well.



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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

Summary

Rule	Number of secrets leaked
Dominios expuestos	4

Passwords detected in commit history

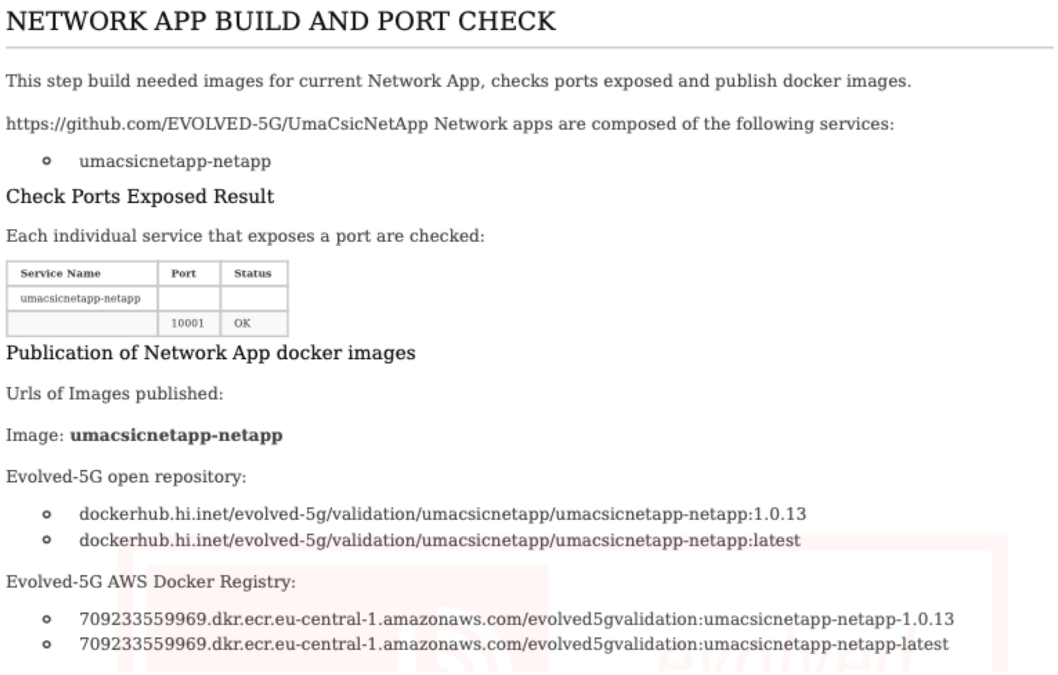
Severity	Description	Match	File	Author	Date
low	Dominios expuestos	ttp://umacsic-nef.apps.ocp-epg.hi.inet	k8s/netapp/environment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/environment.yaml#L12-L12)	Evolved5G	2023-09-26 09:31
low	Dominios expuestos	T: "umacsic-capif.apps.ocp-epg.hi.inet	k8s/netapp/environment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/environment.yaml#L15-L15)	Evolved5G	2023-09-26 09:31
low	Dominios expuestos	- umacsic-nef.apps.ocp-epg.hi.inet	k8s/netapp/deployment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/deployment.yaml#L124-L124)	Evolved5G	2023-09-26 09:31
low	Dominios expuestos	- umacsic-capif.apps.ocp-epg.hi.inet	k8s/netapp/deployment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/deployment.yaml#L125-L125)	Evolved5G	2023-09-26 09:31

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/UmaCsicNetApp/wiki/secrets-Telefonica-Evolved5g-UmaCsicNetApp

Figure 27 Source Code Secrets Analysis Report Page

Step 3 – Network App Build and Port Check: Once the source code has been analysed, Network App container images needs to be built and connectivity specified for the Network Apps checked. This is performed in this step, container images are built and uploaded to both EVOLVED-5G Repository (Artifactory) and to the Docker registry in AWS. URLs for generated containers are included in the report. Additionally, open ports declared by the Network Apps are verified to validate that connectivity with the Network App will be working properly once deployed.



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/UmaCsicNetApp Network apps are composed of the following services:

- umacsicnetapp-netapp

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
umacsicnetapp-netapp		
	10001	OK

Publication of Network App docker images

Urls of Images published:

Image: **umacsicnetapp-netapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/umacsicnetapp/umacsicnetapp-netapp:1.0.13
- dockerhub.hi.inet/evolved-5g/validation/umacsicnetapp/umacsicnetapp-netapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:umacsicnetapp-netapp-1.0.13
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:umacsicnetapp-netapp-latest

Figure 28 Network App Build and Port Check

Step 4 - Image Security Analysis: In this step, the generated binary images of the Network App are analysed for security vulnerabilities. This step is mandatory as the container images contain not only Network App code but Operative System and libraries that have not been analysed in Step 1. Vulnerabilities can be detected in Libraries used by the Network App that jeopardize the security of the container image in a production environment. One report page is generated per container image of the Network Application. When CRITICAL vulnerabilities are detected, the test is reported as FAILURE for the Network App developer to solve CRITICAL vulnerabilities detected.

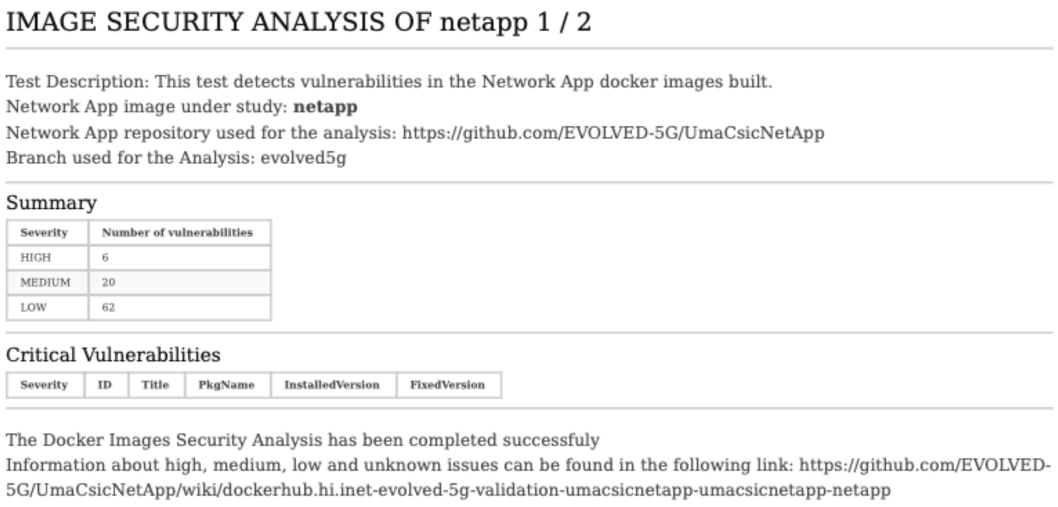


IMAGE SECURITY ANALYSIS OF netapp 1 / 2

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

Summary

Severity	Number of vulnerabilities
HIGH	6
MEDIUM	20
LOW	62

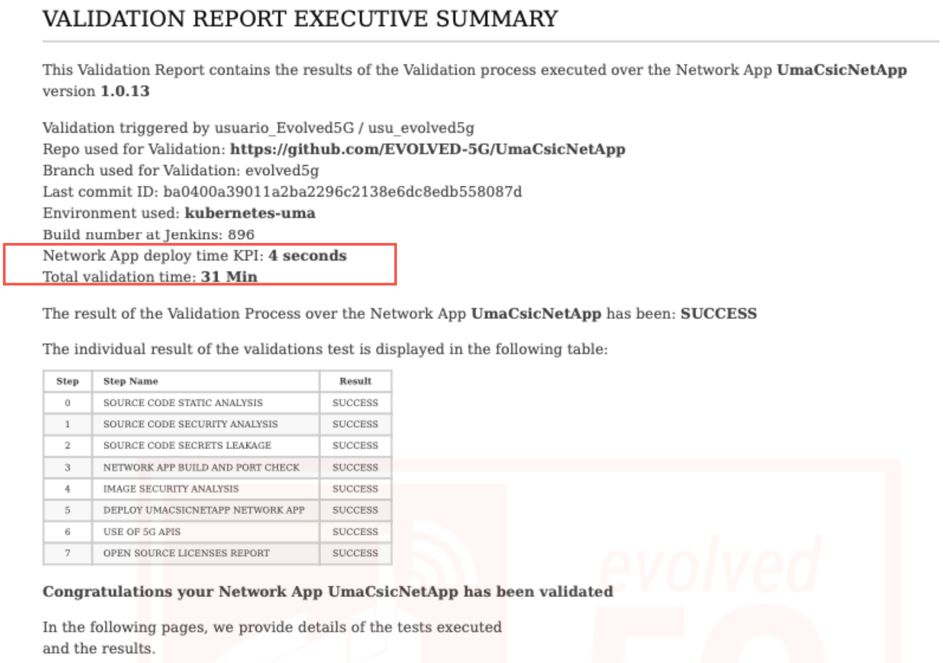
Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion

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/UmaCsicNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-umacsicnetapp-umacsicnetapp-netapp

Figure 29 Container Image Security Analysis Report Page

Step 5 – Deploy the Network Application: Once the Network Application images have been proved secured, the Network Application is deployed in Kubernetes infrastructure to execute the next steps. The deployment time KPI is reported in the Summary page as displayed in the following picture:



VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **UmaCsicNetApp** version **1.0.13**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/UmaCsicNetApp**
Branch used for Validation: evolved5g
Last commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d
Environment used: **kubernetes-uma**
Build number at Jenkins: 896
Network App deploy time KPI: **4 seconds**
Total validation time: **31 Min**

The result of the Validation Process over the Network App **UmaCsicNetApp** has been: **SUCCESS**

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

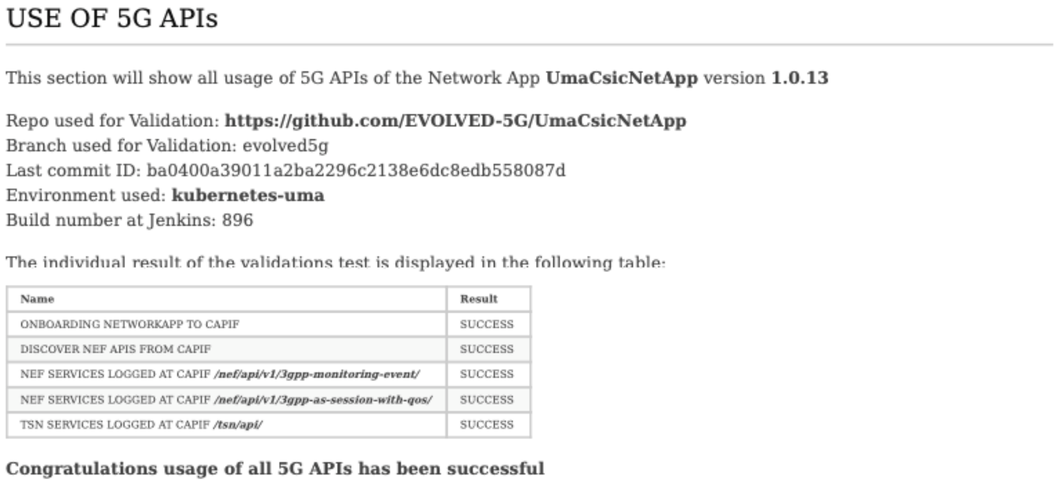
Step	Step Name	Result
0	SOURCE CODE STATIC ANALYSIS	SUCCESS
1	SOURCE CODE SECURITY ANALYSIS	SUCCESS
2	SOURCE CODE SECRETS LEAKAGE	SUCCESS
3	NETWORK APP BUILD AND PORT CHECK	SUCCESS
4	IMAGE SECURITY ANALYSIS	SUCCESS
5	DEPLOY UMACSICNETAPP NETWORK APP	SUCCESS
6	USE OF 5G APIS	SUCCESS
7	OPEN SOURCE LICENSES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

Congratulations your Network App UmaCsicNetApp has been validated

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

Figure 30 Summary of the Validation Report containing the Deployment Time KPI

Step 6 – Usage of 5G APIs. This step is corner stone of EVOLVED-5G project. It reports the usage of 5G Platform APIs integrated in the Network Application. 5G APIs are typically NEF APIs and TSN APIs that, in EVOLVED5G are exposed using CAPIF. On one hand, CAPIF integration is tested to do the Onboarding in CAPIF but also Discover the NEF and TSN APIs using CAPIF. Once NEF and TSN APIs have been discovered by the Network Applications, NEF and TSN Endpoints are consumed by the Network Applications. Both NEF Emulator and TSN Application Function report API usage to CAPIF using the Logging API capability in CAPIF Core Function. This method for reporting API usage is convenient as it is Extendible to any other API that in the future would be added to EVOLVED-5G test suite.



USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **UmaCsicNetApp** version **1.0.13**

Repo used for Validation: **https://github.com/EVOLVED-5G/UmaCsicNetApp**
Branch used for Validation: evolved5g
Last commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d
Environment used: **kubernetes-uma**
Build number at Jenkins: 896

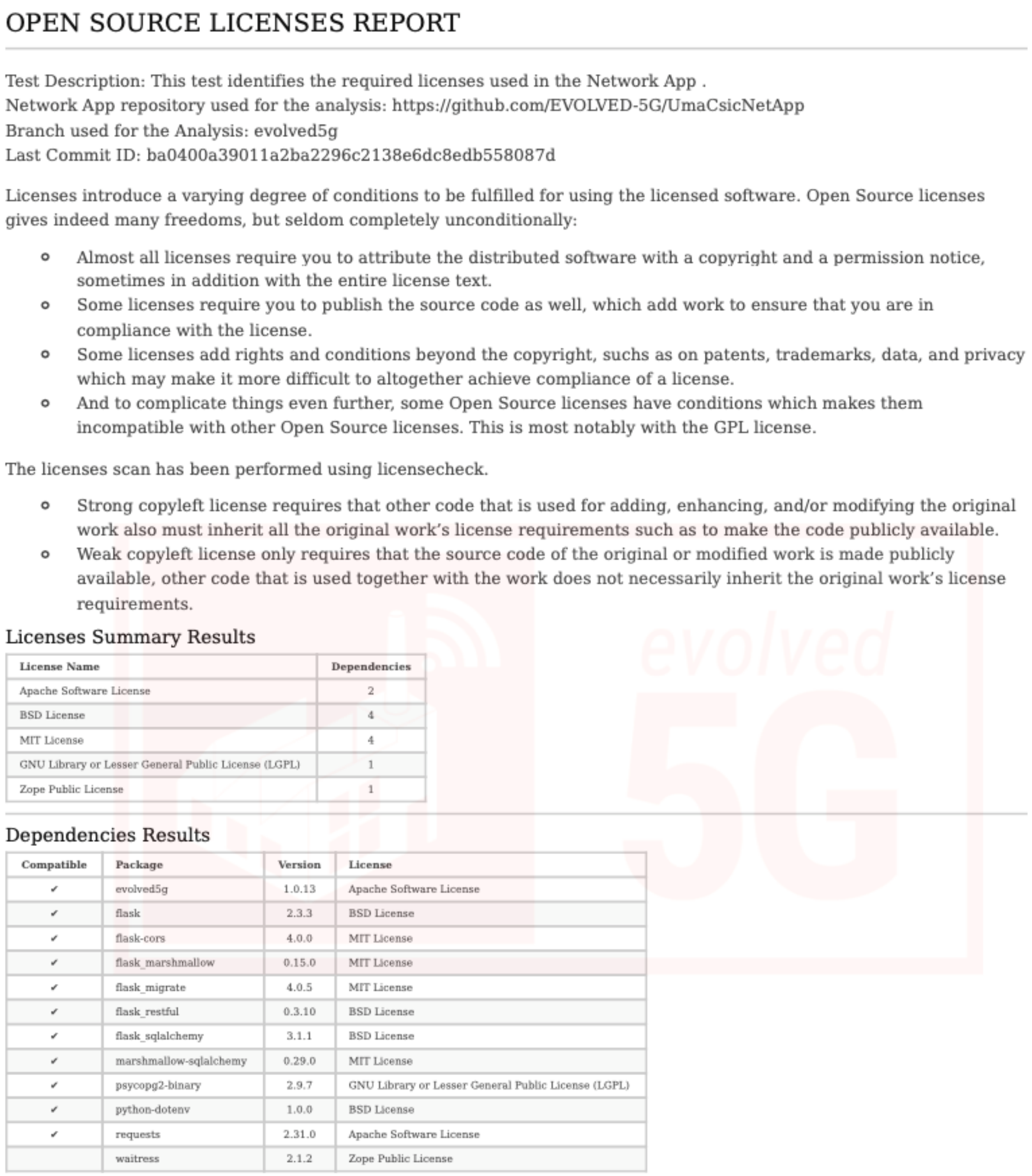
The individual result of the validations test is displayed in the following table:

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

Congratulations usage of all 5G APIs has been successful

Figure 31 5G API Usage Analysis Report Page

Step 7 – Open-Source License Report: Final step is to collect information about open-source Licenses used by the Network Application. Though initially was selected Debriked [18] as the tool to report this information, a License change in Debriked during the project force us to change to use Licensecheck [19] tool instead, that offers similar information. This last-minute change reveals the flexibility and adaptability of the EVOLVED-5G Validation environment and the integration facilities to adapt new tools. The information provided is informative both for Developers and for potential users of the Network Applications.



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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

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
Apache Software License	2
BSD License	4
MIT License	4
GNU Library or Lesser General Public License (LGPL)	1
Zope Public License	1

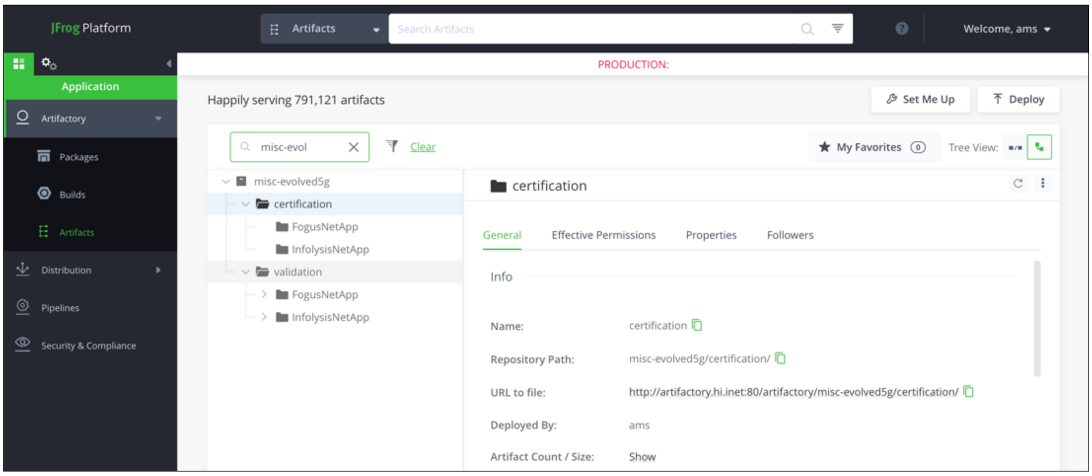
Dependencies Results

Compatible	Package	Version	License
✓	evolved5g	1.0.13	Apache Software License
✓	flask	2.3.3	BSD License
✓	flask-cors	4.0.0	MIT License
✓	flask_marshmallow	0.15.0	MIT License
✓	flask_migrate	4.0.5	MIT License
✓	flask_restful	0.3.10	BSD License
✓	flask_sqlalchemy	3.1.1	BSD License
✓	marshmallow-sqlalchemy	0.29.0	MIT License
✓	psycopg2-binary	2.9.7	GNU Library or Lesser General Public License (LGPL)
✓	python-dotenv	1.0.0	BSD License
✓	requests	2.31.0	Apache Software License
	waitress	2.1.2	Zope Public License

Figure 32 Open-Source Licenses Analysis Report Page

4.2.2 Open-repository onboarding

Upon completion of the process, images generated will be uploaded, along with the results of the validation to Artifactory Validation folder. Later, in order to continue with the required Network App certification procedure, the Certification Process will retrieve the Network App image from the Validation folder in Artifactory.



PRODUCTION:

Happily serving 791,121 artifacts

Name: certification

Repository Path: misc-evolved5g/certification/

URL to file: http://artifactory.hi.inet:80/artifactory/misc-evolved5g/certification/

Deployed By: ams

Artifact Count / Size: Show

Figure 33 Validated image onboarded to Open-Repository

Only Validated Network Apps will be suitable to being pushed to the Certification Phase. This is a condition established by EVOLVED-5G by design and based on the rationale that Certification resources will have significant costs, and going through a successful validation of the Network App guarantees that chances of Network App being certified will be higher.

5 Validation Rounds and Overall results

The primary objective of the Validation environment is to provide the essential tools and methodologies necessary for conducting the validation process. This process encompasses the evaluation of the functionality of Network Apps when they are used in conjunction with their respective vApps. Within the framework of the EVOLVED-5G project the overarching goal is to demonstrate that these vApps meet the desired performance criteria as defined by the respective vertical/SME, while leveraging the capabilities of the Network Apps. Moreover, when a Network App is validated alongside a vApp, it ensures that the Network App can function optimally under genuine network conditions, assuming that the vApp fully leverages all the capabilities provided by the Network App.

In this sense recognizing the need for a holistic approach towards the validation phase, two rounds of validation were conducted in the EVOLVED-5G platforms (Athens and Malaga) to emphasize and defend the aforementioned critical aspects. The active participation of SMEs in the two rounds of the validation phase, proved immensely advantageous for both the EVOLVED-5G ecosystem and the SMEs themselves. First, it led to the identification of areas for improvement on both the Network Apps and the validation pipeline side, fostering evolution and enhancements towards the overall process and outcome.

Furthermore, the overall success of these tests not only demonstrated and harnessed the technical expertise of the participants involved in the process, but also highlighted the practical advantages of integrating all the steps composing the validation process in an automated way.

In the previous section, the steps comprising the validation pipeline at its final stage were described, which basically reflect the essential process that Network Applications must undergo for successful validation. In the following subsection, a summary of the results towards the successful validation of Network Apps for each of the two rounds is provided.

5.1 First Round of Validation

The initial round of testing utilized the version 4 of the Network Apps (as described in Deliverable 4.3), while the subsequent and final round was conducted using the final version. During the first round of running the validation pipeline the SMEs selected to run the pipeline either on one of the provided infrastructures or to test them both so as to have a holistic approach and view. The following table presents the selection of the platform(s) per SME/Network App.

Table 8 Results of the first round of validation process

SME/Network App	Validation pipeline Malaga	Validation pipeline Athens
IMM -*Remote assistance in AR Network App*	✓	
GMI -*Digital/physical twin Network App*		✓
INF -*Chatbot assistant Network App*		✓
CAF - *NetMapper Network App*		
ININ -*Industrial grade 5G connectivity Network App*		✓
ZORTENET - *Anomaly Detection Network App*		✓

CSIC/UMA -*Smart irrigation 5G Agriculture Network App*	✓	✓
8BELLS -*Traffic Management Network App*	✓	
FOGUS -*5G SIEM Network App*		✓
IQBIT -*ID Management and Access Control Network App*	✓	✓
PAL -*Teleoperation Network App*	✓	
UMS/PAL -*Localisation Network App*	✓	

5.2 Second Round of Validation

In preparation for the validation process and the utilisation of the validation pipeline for the final round, additional configurations were made on the Network App side by the SMEs. This included updating with the final version of the SDK provided by the project, enabling interested Network Apps to incorporate the TSN capabilities among others, which is also considered as a step of the validation process. As presented in the table below, all the Network Apps have successfully completed the validation process (the final validation reports are provided in Annex). The last round of validation tests using the pipeline has been completed on Malaga's platform for all the SMEs.

Table 9 Results for the second (final) round of the validation process

Pillar	SME	Network App Name	Validation Pipeline Test
Interaction of Employees and Machines (IEM)	IMM	*Remote assistance in AR Network App*	✓
			✓
	INF	*Chatbot assistant Network App*	✓
	GMI-Aero	*Digital/physical twin Network App*	✓
Factory of the Future pillar (FoF)	CAF	*NetMapper Network App*	✓
	ININ	*Industrial grade 5G connectivity Network App*	✓
	UMA	*Smart irrigation 5G Agriculture Network App*	✓
	ZORTENET	*Anomaly Detection Network App*	✓
Security Guarantees and	8BELLS	*Traffic Management Network App*	✓

risk Analysis Pillar (SEC)	IQBIT	*ID Management and Access Control Network App*	✓
	FOGUS	*5G SIEM Network App*	✓
Production Line Infrastructure Pillar (PLI)	PAL	*Teleoperation Network App*	✓
	UMS/PAL	*Localisation Network App*	✓

6 CONCLUSION

This deliverable provides a detailed description of the work conducted within the scope of WP5, specifically focusing on Task 5.2 Network Apps Validation and Onboarding to the Open Repository, which is driving the content of this deliverable. The primary objective of Task 5.2, throughout the project's duration, is to define the process and establish validation tests for all Network Apps. This has been achieved through close collaboration with WP3 and WP4, utilizing tools developed in the former and the final prototypes from the latter.

In this context the content of the deliverable has been shaped based on the premises. More specifically, Section 2 presents the status and updates made to the validation framework in comparison to the initial version provided in D5.2. This environment has been instrumental in executing the final validation tests for the Network Apps. Specifically, this section addresses updates related to the CI/CD tools and the Kubernetes clusters of the EVOLVED-5G platforms in Athens-Malaga respectively. Section 3 outlines the process for measuring specific Key Performance Indicators (KPIs) of the Network Apps. This process aims to showcase that the each vApp achieves the desired performance levels while effectively utilizing the capabilities of the respective Network App. Taking a step further, Section 4 describes the stages comprising the validation process for the Network Apps and evaluates the results. The overall rationale behind conducting two rounds of validation is provided in Section 5.

With the successful completion of the validation process, as indicated by the comprehensive validation reports provided in Annex 1 and Annex 2, the Network Apps are now ready to undergo the certification process. The final goal is to prepare these validated and later certified Network Apps for uploading to the marketplace, making them accessible to a wider audience and ensuring their seamless integration into the evolving technological landscape.

7 REFERENCES

[1] EVOLVED-5G, "NetApps Validation and onboarding to Open Repository (intermediate)".

[2] EVOLVED-5G, "Deliverable D3.2 “NetApp Certification Tools and Marketplace development(intermediate) https://evolved-5g.eu/wp-content/uploads/2022/07/EVOLVED-5G-D3.2_FINAL.pdf".

[3] EVOLVED-5G, "Network Apps Certification Tools and Marketplace development (https://evolved-5g.eu/wp-content/uploads/2023/09/EVOLVED-5G-D3.4_FINAL.pdf)".

[4] "D3.3 Implementations and integrations towards EVOLVED-5G framework realisation -final (https://evolved-5g.eu/wp-content/uploads/2023/05/EVOLVED-5G-D3.3_FV.pdf)".

[5] "Deliverable 4.4 Network Apps for Interaction of Employees and Machines (https://evolved-5g.eu/wp-content/uploads/2023/09/EVOLVED-5G_D4.4_Final.pdf)".

[6] "MetalLB, bare metal load-balancer for Kubernetes, from https://metallb.universe.tf/," [Online].

[7] "Containerd from https://containerd.io/," [Online].

[8] "KubeVirt from https://kubevirt.io/," [Online].

[9] "RobotFramework, from https://robotframework.org/robotframework/," [Online].

[10] [Online]. Available: https://www.sonarqube.org/.

[11] [Online]. Available: https://robotframework.org/.

[12] 3GPP, "TS 23.222 Common API Framework for 3GPP Northbound APIs," [Online].

[13] 3GPP, "TS 29.522 "5G System; Network Exposure Function Northbound APIs; Stage 3", Release 15, v17.6.0," https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3437, June 2022.

[14] "3GPP TS 33.122 Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[15] 3GPP, "TS 29.122 "T8 reference point for Northbound APIs", Release 15, v17.6.0, June 2022," [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3239.

[16] "Helm The package Manager for Kubernetes from https://helm.sh/," [Online].

[17] "Trivy project, from https://aquasecurity.github.io/trivy/v0.28.1/," [Online].

[18] "Debriked project, from https://debricked.com/tools/license-compliance/," [Online].

[19] [Online]. Available: Licensecheck from https://github.com/google/licensecheck.

[20] "D4. 3 5G Exposure Capabilities for Vertical Applications (Final) (https://evolved-5g.eu/wp-content/uploads/2023/09/EVOLVED-5G-D4.3-v1.1_final_ncsrd.pdf)".

8 ANNEXES

ANNEX – VALIDATION REPORTS

Network App Validation Report: ImmersionNetApp

Date: 25/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **ImmersionNetApp** version **4.1**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/ImmersionNetApp**
Branch used for Validation: evolved5g
Last commit ID: 52fc6f0219879dded4a9550a103b85831ef4a06c
Environment used: **kubernetes-uma**
Build number at Jenkins: 888
Network App deploy time KPI: **27 seconds**
Total validation time: **32 Min**

The result of the Validation Process over the Network App **ImmersionNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App ImmersionNetApp has been validated

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

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/ImmersionNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 52fc6f0219879dded4a9550a103b85831ef4a06c

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

Scan of immersionnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	3
major	18
minor	30

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-immersionnetapp-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/ImmersionNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 52fc6f0219879dded4a9550a103b85831ef4a06c

The security scan has been performed using Trivy version 0.35.0

Scan of repo: ImmersionNetApp

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/ImmersionNetApp/wiki/Telefonica-Evolved5g-ImmersionNetApp

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/ImmersionNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 52fc6f0219879dded4a9550a103b85831ef4a06c

Summary

Rule	Number of secrets leaked
Dominios expuestos	20

Passwords detected in commit history

Severity	Description	Match	File	Author
low	Dominios expuestos	localization-nef.apps.ocp-epg.hi.inet	K8s/OLD_Capif_and_nef/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/OLD_Capif_and_nef/environment.yaml#L18-L18)	Evolved5G
low	Dominios expuestos	ocalization-capif.apps.ocp-epg.hi.inet	K8s/OLD_Capif_and_nef/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/OLD_Capif_and_nef/environment.yaml#L23-L23)	Evolved5G
low	Dominios expuestos	IP: immersion-nef.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/environment.yaml#L13-L13)	Evolved5G
low	Dominios expuestos	p://immersion-nef.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/environment.yaml#L17-L17)	Evolved5G
low	Dominios expuestos	: immersion-capif.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/environment.yaml#L22-L22)	Evolved5G
low	Dominios expuestos	: immersion-capif.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/environment.yaml#L25-L25)	Evolved5G
low	Dominios expuestos	T: immsersion-tsn.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/environment.yaml#L27-L27)	Evolved5G
low	Dominios expuestos	p://immersion-nef.apps.ocp-epg.hi.inet	src/python/emulator/Emulator_Utils.py (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/src/python/emulator/Emulator_Utils.py#L27-L27)	Evolved5G
low	Dominios expuestos	- immersion-nef.apps.ocp-epg.hi.inet	K8s/deployment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/deployment.yaml#L133-L133)	Evolved5G
low	Dominios expuestos	- immersion-capif.apps.ocp-epg.hi.inet	K8s/deployment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/deployment.yaml#L134-L134)	Evolved5G
low	Dominios expuestos	- immsersion-tsn.apps.ocp-epg.hi.inet	K8s/deployment.yaml (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/730a6287e801a45c89f7cd3e05d355b2c2adab0d/K8s/deployment.yaml#L135-L135)	Evolved5G
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-ImmersionNetApp/blob/29d564474fdf4a867f50ca5a12d6e91f0be2a80d/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez

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/ImmersionNetApp/wiki/secrets-Telefonica-Evolved5g-ImmersionNetApp

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/ImmersionNetApp Network apps are composed of the following services:

- immersionnetapp-imm_netapp_container

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
immersionnetapp-imm_netapp_container		
	9876	OK
	9877	OK
	9988	OK
	9998	OK
	9999	OK

Publication of Network App docker images

Urls of Images published:

Image: **immersionnetapp-imm_netapp_container**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/immersionnetapp/immersionnetapp-imm_netapp_container:4.1
- dockerhub.hi.inet/evolved-5g/validation/immersionnetapp/immersionnetapp-imm_netapp_container:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:immersionnetapp-imm_netapp_container-4.1
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:immersionnetapp-imm_netapp_container-latest

IMAGE SECURITY ANALYSIS OF imm_netapp_container 1 / 1

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

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	63
MEDIUM	218
LOW	494

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-25775 (https://nvd.nist.gov/vuln/detail/CVE-2023-25775)	Improper access control	linux-libc-dev	6.1.52-1	
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	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:9.2p1-2	

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/ImmersionNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-immersionnetapp-immersionnetapp-imm_netapp_container

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **ImmersionNetApp** version **4.1**

Repo used for Validation: **https://github.com/EVOLVED-5G/ImmersionNetApp**
Branch used for Validation: evolved5g
Last commit ID: 52fc6f0219879dded4a9550a103b85831ef4a06c
Environment used: **kubernetes-uma**
Build number at Jenkins: 888

The individual result of the validations test is 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-monitoring-event/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

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/ImmersionNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 52fc6f0219879dded4a9550a103b85831ef4a06c

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
Historical Permission Notice and Disclaimer (HPND)	1
Apache Software License	1
BSD License	3
MIT License	1

Dependencies Results

Compatible	Package	Version	License
✔	Pillow	9.2.0	Historical Permission Notice and Disclaimer (HPND)
✔	evolved5g	1.0.13	Apache Software License
✔	flask	2.3.3	BSD License
✔	jsonpickle	3.0.2	BSD License
✔	python-dotenv	1.0.0	BSD License
✔	python-statemachine	2.1.1	MIT License

evolved 5G

Network App Validation Report: GmiAeroNetApp

Date: 28/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **GmiAeroNetApp** version **4.0**

Validation triggered by JORGE / jms
Repo used for Validation: **https://github.com/EVOLVED-5G/GmiAeroNetApp**
Branch used for Validation: evolved5g
Last commit ID: e36888017c7bac5748a51a65fdeb740b6370f112
Environment used: **kubernetes-athens**
Build number at Jenkins: 932
Network App deploy time KPI: **9 seconds**
Total validation time: **37 Min**

The result of the Validation Process over the Network App **GmiAeroNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App GmiAeroNetApp has been validated

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

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/GmiAeroNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e36888017c7bac5748a51a65fdeb740b6370f112

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

Scan of gmiaeronetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	3
major	25
minor	27

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-gmiaeronetapp-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/GmiAeroNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e36888017c7bac5748a51a65fdeb740b6370f112

The security scan has been performed using Trivy version 0.35.0

Scan of repo: GmiAeroNetApp

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/GmiAeroNetApp/wiki/Telefonica-Evolved5g-GmiAeroNetApp

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/GmiAeroNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e36888017c7bac5748a51a65fdeb740b6370f112

Summary

Rule	Number of secrets leaked
Dominios expuestos	18

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/iac/terraform/main.tf#L12-L12)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/iac/slave/Dockerfile#L4-L4)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/iac/slave/Dockerfile#L77-L77)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/pac/Jenkins-deploy.groovy#L13-L13)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/pac/Jenkins-destroy.groovy#L13-L13)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/pac/Jenkins-build.groovy#L43-L43)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/pac/Jenkins-build.groovy#L44-L44)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/pac/Jenkins-build.groovy#L45-L45)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/3bc34ab118c5013f95dda750e8fa9642bdc58c4c/pac/Jenkins-build.groovy#L46-L46)	Evolved5G	2023-06-01 10:24
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-09-19 10:54
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-GmiAeroNetApp/blob/f9c63e3635201f18e8fa1c881a416a51e87a1b55/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 10:54

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/GmiAeroNetApp/wiki/secrets-Telefonica-Evolved5g-GmiAeroNetApp

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/GmiAeroNetApp Network apps are composed of the following services:

- gmiaeronetapp-gmi_netapp_container

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
gmiaeronetapp-gmi_netapp_container		
	8383	OK

Publication of Network App docker images

Urls of Images published:

Image: **gmiaeronetapp-gmi_netapp_container**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/gmiaeronetapp/gmiaeronetapp-gmi_netapp_container:4.0
- dockerhub.hi.inet/evolved-5g/validation/gmiaeronetapp/gmiaeronetapp-gmi_netapp_container:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:gmiaeronetapp-gmi_netapp_container-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:gmiaeronetapp-gmi_netapp_container-latest

IMAGE SECURITY ANALYSIS OF gmi_netapp_container 1 / 2

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

Summary

Severity	Number of vulnerabilities
CRITICAL	88
HIGH	726
MEDIUM	946
LOW	827
UNKNOWN	9

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2021-22945 (https://nvd.nist.gov/vuln/detail/CVE-2021-22945)	curl: use-after-free and double-free in MQTT sending	curl	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32207 (https://nvd.nist.gov/vuln/detail/CVE-2022-32207)	Unpreserved file permissions	curl	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	curl	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u5
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	curl	7.74.0-1.3+deb11u1	
CRITICAL	CVE-2022-1664 (https://nvd.nist.gov/vuln/detail/CVE-2022-1664)	Dpkg::Source::Archive in dpkg, the Debian package management system, b ...	dpkg	1.20.9	1.20.10
CRITICAL	CVE-2022-1664 (https://nvd.nist.gov/vuln/detail/CVE-2022-1664)	Dpkg::Source::Archive in dpkg, the Debian package management system, b ...	dpkg-dev	1.20.9	1.20.10
CRITICAL	CVE-2022-23521 (https://nvd.nist.gov/vuln/detail/CVE-2022-23521)	git: gitattributes parsing integer overflow	git	1:2.30.2-1	1:2.30.2-1+deb11u1
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	1:2.30.2-1	1:2.30.2-1+deb11u1
CRITICAL	CVE-2022-23521 (https://nvd.nist.gov/vuln/detail/CVE-2022-23521)	git: gitattributes parsing integer overflow	git-man	1:2.30.2-1	1:2.30.2-1+deb11u1
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	1:2.30.2-1	1:2.30.2-1+deb11u1
CRITICAL	CVE-2021-30473 (https://nvd.nist.gov/vuln/detail/CVE-2021-30473)	aom_image.c in libaom in AOMedia before 2021-04-07 frees memory that i ...	libaom0	1.0.0.errata1-3	1.0.0.errata1-3+deb11u1
CRITICAL	CVE-2021-30474 (https://nvd.nist.gov/vuln/detail/CVE-2021-30474)	aom_dsp/grain_table.c in libaom in AOMedia before 2021-03-30 has a use ...	libaom0	1.0.0.errata1-3	1.0.0.errata1-3+deb11u1
CRITICAL	CVE-2021-30475 (https://nvd.nist.gov/vuln/detail/CVE-2021-30475)	aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buf ...	libaom0	1.0.0.errata1-3	1.0.0.errata1-3+deb11u1
CRITICAL	CVE-2022-24963 (https://nvd.nist.gov/vuln/detail/CVE-2022-24963)	integer overflow/wraparound in apr_encode	libapr1	1.7.0-6+deb11u1	1.7.0-6+deb11u2
CRITICAL	CVE-2021-43400 (https://nvd.nist.gov/vuln/detail/CVE-2021-43400)	bluez: use-after-free in gatt-database.c	libbluetooth-dev	5.55-3.1	
CRITICAL	CVE-2021-43400 (https://nvd.nist.gov/vuln/detail/CVE-2021-43400)	bluez: use-after-free in gatt-database.c	libbluetooth3	5.55-3.1	
CRITICAL	CVE-2021-33574 (https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	mq_notify does not handle separately allocated thread attributes	libc-bin	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
CRITICAL	CVE-2021-33574 (https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	mq_notify does not handle separately allocated thread attributes	libc6	2.31-13+deb11u2	2.31-13+deb11u3
CRITICAL	CVE-2022-23218 (https://nvd.nist.gov/vuln/detail/CVE-2022-23218)	Stack-based buffer overflow in svcunix_create via long pathnames	libc6	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
	CVE-2021-33574	mq_notify does not handle separately allocated thread			2.31-

CRITICAL	(https://nvd.nist.gov/vuln/detail/CVE-2021-33574)	attributes	libc6-dev	2.31-13+deb11u2	13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
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	2.31-13+deb11u2	2.31-13+deb11u3
CRITICAL	CVE-2021-22945 (https://nvd.nist.gov/vuln/detail/CVE-2021-22945)	curl: use-after-free and double-free in MQTT sending	libcurl3-gnutls	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32207 (https://nvd.nist.gov/vuln/detail/CVE-2022-32207)	Unpreserved file permissions	libcurl3-gnutls	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	libcurl3-gnutls	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u5
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	libcurl3-gnutls	7.74.0-1.3+deb11u1	
CRITICAL	CVE-2021-22945 (https://nvd.nist.gov/vuln/detail/CVE-2021-22945)	curl: use-after-free and double-free in MQTT sending	libcurl4	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32207 (https://nvd.nist.gov/vuln/detail/CVE-2022-32207)	Unpreserved file permissions	libcurl4	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	libcurl4	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u5
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	libcurl4	7.74.0-1.3+deb11u1	
CRITICAL	CVE-2021-22945 (https://nvd.nist.gov/vuln/detail/CVE-2021-22945)	curl: use-after-free and double-free in MQTT sending	libcurl4-openssl-dev	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32207 (https://nvd.nist.gov/vuln/detail/CVE-2022-32207)	Unpreserved file permissions	libcurl4-openssl-dev	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
CRITICAL	CVE-2022-32221 (https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	libcurl4-openssl-dev	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u5
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	libcurl4-openssl-dev	7.74.0-1.3+deb11u1	
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+dfsg1-0.8	
CRITICAL	CVE-2019-8457 (https://nvd.nist.gov/vuln/detail/CVE-2019-8457)	heap out-of-bound read in function rtreenode()	libdb5.3-dev	5.3.28+dfsg1-0.8	
CRITICAL	CVE-2022-1253 (https://nvd.nist.gov/vuln/detail/CVE-2022-1253)	Heap-based Buffer Overflow in GitHub repository strukturag/libde265 pr ...	libde265-0	1.0.8-1	1.0.11-0+deb11u1
CRITICAL	CVE-2022-1664 (https://nvd.nist.gov/vuln/detail/CVE-2022-1664)	Dpkg::Source::Archive in dpkg, the Debian package management system, b ...	libdpkg-perl	1.20.9	1.20.10
CRITICAL	CVE-2022-22822 (https://nvd.nist.gov/vuln/detail/CVE-2022-22822)	Integer overflow in addBinding in xmlparse.c	libexpat1	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-22823 (https://nvd.nist.gov/vuln/detail/CVE-2022-22823)	Integer overflow in build_model in xmlparse.c	libexpat1	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-22824 (https://nvd.nist.gov/vuln/detail/CVE-2022-22824)	Integer overflow in defineAttribute in xmlparse.c	libexpat1	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-23852 (https://nvd.nist.gov/vuln/detail/CVE-2022-23852)	Integer overflow in function XML_GetBuffer	libexpat1	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-25235 (https://nvd.nist.gov/vuln/detail/CVE-2022-25235)	Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution	libexpat1	2.2.10-2	2.2.10-2+deb11u2
CRITICAL	CVE-2022-25236 (https://nvd.nist.gov/vuln/detail/CVE-2022-25236)	prefix]" attribute values can lead to arbitrary code execution	libexpat1	2.2.10-2	2.2.10-2+deb11u2
CRITICAL	CVE-2022-25315 (https://nvd.nist.gov/vuln/detail/CVE-2022-25315)	Integer overflow in storeRawNames()	libexpat1	2.2.10-2	2.2.10-2+deb11u2
CRITICAL	CVE-2022-22822 (https://nvd.nist.gov/vuln/detail/CVE-2022-22822)	Integer overflow in addBinding in xmlparse.c	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-22823 (https://nvd.nist.gov/vuln/detail/CVE-2022-22823)	Integer overflow in build_model in xmlparse.c	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-22824 (https://nvd.nist.gov/vuln/detail/CVE-2022-22824)	Integer overflow in defineAttribute in xmlparse.c	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-23852 (https://nvd.nist.gov/vuln/detail/CVE-2022-23852)	Integer overflow in function XML_GetBuffer	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u1
CRITICAL	CVE-2022-25235 (https://nvd.nist.gov/vuln/detail/CVE-2022-25235)	Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u2
CRITICAL	CVE-2022-25236 (https://nvd.nist.gov/vuln/detail/CVE-2022-25236)	prefix]" attribute values can lead to arbitrary code execution	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u2
CRITICAL	CVE-2022-25315 (https://nvd.nist.gov/vuln/detail/CVE-2022-25315)	Integer overflow in storeRawNames()	libexpat1-dev	2.2.10-2	2.2.10-2+deb11u2
CRITICAL	CVE-2022-27404 (https://nvd.nist.gov/vuln/detail/CVE-2022-27404)	Buffer overflow in sfnt_init_face	libfreetype-dev	2.10.4+dfsg-1	2.10.4+dfsg-1+deb11u1
CRITICAL	CVE-2022-27404 (https://nvd.nist.gov/vuln/detail/CVE-2022-27404)	Buffer overflow in sfnt_init_face	libfreetype6	2.10.4+dfsg-1	2.10.4+dfsg-1+deb11u1
CRITICAL	CVE-2022-27404 (https://nvd.nist.gov/vuln/detail/CVE-2022-27404)	Buffer overflow in sfnt_init_face	libfreetype6-dev	2.10.4+dfsg-1	2.10.4+dfsg-1+deb11u1

CRITICAL	CVE-2022-3515 (https://nvd.nist.gov/vuln/detail/CVE-2022-3515)	integer overflow may lead to remote code execution	libksba8	1.5.0-3	1.5.0-3+deb11u1
CRITICAL	CVE-2022-47629 (https://nvd.nist.gov/vuln/detail/CVE-2022-47629)	integer overflow to code execution	libksba8	1.5.0-3	1.5.0-3+deb11u2
CRITICAL	CVE-2022-29155 (https://nvd.nist.gov/vuln/detail/CVE-2022-29155)	OpenLDAP SQL injection	libldap-2.4-2	2.4.57+dfsg-3	2.4.57+dfsg-3+deb11u1
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	Out-of-bounds read in compile_xclass_matchingpath in pcre2_jit_compile.c	libpcre2-16-0	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1587 (https://nvd.nist.gov/vuln/detail/CVE-2022-1587)	Out-of-bounds read in get_recurse_data_length in pcre2_jit_compile.c	libpcre2-16-0	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	Out-of-bounds read in compile_xclass_matchingpath in pcre2_jit_compile.c	libpcre2-32-0	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1587 (https://nvd.nist.gov/vuln/detail/CVE-2022-1587)	Out-of-bounds read in get_recurse_data_length in pcre2_jit_compile.c	libpcre2-32-0	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	Out-of-bounds read in compile_xclass_matchingpath in pcre2_jit_compile.c	libpcre2-8-0	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1587 (https://nvd.nist.gov/vuln/detail/CVE-2022-1587)	Out-of-bounds read in get_recurse_data_length in pcre2_jit_compile.c	libpcre2-8-0	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	Out-of-bounds read in compile_xclass_matchingpath in pcre2_jit_compile.c	libpcre2-dev	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1587 (https://nvd.nist.gov/vuln/detail/CVE-2022-1587)	Out-of-bounds read in get_recurse_data_length in pcre2_jit_compile.c	libpcre2-dev	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	Out-of-bounds read in compile_xclass_matchingpath in pcre2_jit_compile.c	libpcre2-posix2	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2022-1587 (https://nvd.nist.gov/vuln/detail/CVE-2022-1587)	Out-of-bounds read in get_recurse_data_length in pcre2_jit_compile.c	libpcre2-posix2	10.36-2	10.36-2+deb11u1
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	libpython3.9-minimal	3.9.2-1	
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	libpython3.9-stdlib	3.9.2-1	
CRITICAL	CVE-2022-1292 (https://nvd.nist.gov/vuln/detail/CVE-2022-1292)	c_rehash script allows command injection	libssl-dev	1.1.1k-1+deb11u1	1.1.1n-0+deb11u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	libssl-dev	1.1.1k-1+deb11u1	1.1.1n-0+deb11u3
CRITICAL	CVE-2022-1292 (https://nvd.nist.gov/vuln/detail/CVE-2022-1292)	c_rehash script allows command injection	libssl1.1	1.1.1k-1+deb11u1	1.1.1n-0+deb11u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	libssl1.1	1.1.1k-1+deb11u1	1.1.1n-0+deb11u3
CRITICAL	CVE-2021-46848 (https://nvd.nist.gov/vuln/detail/CVE-2021-46848)	Out-of-bound access in ETYPE_OK	libtasn1-6	4.16.0-2	4.16.0-2+deb11u1
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:8.4p1-5	
CRITICAL	CVE-2022-1292 (https://nvd.nist.gov/vuln/detail/CVE-2022-1292)	c_rehash script allows command injection	openssl	1.1.1k-1+deb11u1	1.1.1n-0+deb11u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	openssl	1.1.1k-1+deb11u1	1.1.1n-0+deb11u3
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	python3.9	3.9.2-1	
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	python3.9-minimal	3.9.2-1	
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-2	1:1.2.11.dfsg-2+deb11u2
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-2	1:1.2.11.dfsg-2+deb11u2

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/GmiAeroNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-gmiaeronetapp-gmiaeronetapp-gmi_netapp_container

IMAGE SECURITY ANALYSIS OF optimistic_turing 2 / 2

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

Summary

Severity	Number of vulnerabilities
CRITICAL	14
HIGH	316
MEDIUM	460
LOW	791
UNKNOWN	6

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	curl	7.74.0-1.3+deb11u7	
CRITICAL	CVE-2021-30473 (https://nvd.nist.gov/vuln/detail/CVE-2021-30473)	aom_image.c in libaom in AOMedia before 2021-04-07 frees memory that i ...	libaom0	1.0.0.errata1-3	1.0.0.errata1-3+deb11u1
CRITICAL	CVE-2021-30474 (https://nvd.nist.gov/vuln/detail/CVE-2021-30474)	aom_dsp/grain_table.c in libaom in AOMedia before 2021-03-30 has a use ...	libaom0	1.0.0.errata1-3	1.0.0.errata1-3+deb11u1
CRITICAL	CVE-2021-30475 (https://nvd.nist.gov/vuln/detail/CVE-2021-30475)	aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buf ...	libaom0	1.0.0.errata1-3	1.0.0.errata1-3+deb11u1
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	libcurl3-gnutls	7.74.0-1.3+deb11u7	
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	libcurl4	7.74.0-1.3+deb11u7	
CRITICAL	CVE-2023-23914 (https://nvd.nist.gov/vuln/detail/CVE-2023-23914)	HSTS ignored on multiple requests	libcurl4-openssl-dev	7.74.0-1.3+deb11u7	
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+dfsg1-0.8	
CRITICAL	CVE-2019-8457 (https://nvd.nist.gov/vuln/detail/CVE-2019-8457)	heap out-of-bound read in function rtreenode()	libdb5.3-dev	5.3.28+dfsg1-0.8	
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	libpython3.9-minimal	3.9.2-1	
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	libpython3.9-stdlib	3.9.2-1	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:8.4p1-5+deb11u1	
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	python3.9	3.9.2-1	
CRITICAL	CVE-2021-29921 (https://nvd.nist.gov/vuln/detail/CVE-2021-29921)	python-ipaddress: Improper input validation of octal strings	python3.9-minimal	3.9.2-1	

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/GmiAeroNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-gmiaeronetapp-gmiaeronetapp-optimistic_turing

USE OF 5G APIs

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

Repo used for Validation: **https://github.com/EVOLVED-5G/GmiAeroNetApp**
Branch used for Validation: evolved5g
Last commit ID: e36888017c7bac5748a51a65fdeb740b6370f112
Environment used: **kubernetes-athens**
Build number at Jenkins: 932

The individual result of the validations test is 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

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/GmiAeroNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e36888017c7bac5748a51a65fdeb740b6370f112

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
Apache Software License	3
MIT License	2
BSD License	1

Dependencies Results

Compatible	Package	Version	License
✔	aiofiles	23.2.1	Apache Software License
✔	evolved5g	1.0.13	Apache Software License
✔	fastapi	0.103.1	MIT License
✔	pydantic	2.4.2	MIT License
✔	requests	2.31.0	Apache Software License
✔	uvicorn	0.23.2	BSD License

evolved 5G

Network App Validation Report: InfolysisNetApp

Date: 26/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **InfolysisNetApp** version **4.0**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com//EVOLVED-5G/InfolysisNetApp**
Branch used for Validation: evolved5g
Last commit ID: 7f10808ac5d6e04630ecc1f03c12166eec21f0eb
Environment used: **kubernetes-uma**
Build number at Jenkins: 899
Network App deploy time KPI: **52 seconds**
Total validation time: **37 Min**

The result of the Validation Process over the Network App **InfolysisNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App InfolysisNetApp has been validated

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

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/InfolysisNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 7f10808ac5d6e04630ecc1f03c12166eec21f0eb

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

Scan of infolysisnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	0
major	2
minor	0

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-infolysisnetapp-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/InfolysisNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 7f10808ac5d6e04630ecc1f03c12166eec21f0eb

The security scan has been performed using Trivy version 0.35.0

Scan of repo: InfolysisNetApp

Summary

Severity	Number of vulnerabilities
HIGH	24
MEDIUM	21

Good work. Network App code does not have any security issue.

The Source Code 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/InfolysisNetApp/wiki/Telefonica-Evolved5g-InfolysisNetApp

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/InfolysisNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 7f10808ac5d6e04630ecc1f03c12166eec21f0eb

Summary

Rule	Number of secrets leaked
AWS Access Key	7
Asymmetric Private Key	12
Dominios expuestos	9
Possible WP-config files	1

Passwords detected in commit history

Severity	Description	Match
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
high	AWS Access Key	AIDAQAAAAAAAAABAAIDE
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIICXQIBAAKBgQCzhLXIZCgSvFk6sF0dgKL9pnNPooMkExm8QQ0sslCxz4nnDKjgR7OW1eAy9aXP9NYSyiKeE9o9ijU05nor67Snd8DEC+wPiIMqnZnqkYvfKWFMpRWax8W/Sos
critical	Asymmetric Private Key	--BEGIN PRIVATE KEY-- MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAKulUTZ8B1qccZ8cDXRGSY08gW8KvLlcxxxGC4gZHNT3CBUF8n5R4KE30aZyYZ/rtsQZu05juZJxaJ0qmbe75d
critical	Asymmetric Private Key	--BEGIN PRIVATE KEY-- MIIBSwIBADCCASwGByqGSM44BAEwggEfAoGBAOY0KsTt5EpJ4LtlD3xRS5mDiGE1CMNp0S9X0sK8kP8Aps8iYwMLbZYglk18GCNnCk4SjbAnZHSB3kaIv6AKQc2J8W2YV5se3
critical	Asymmetric Private Key	--BEGIN DSA PRIVATE KEY-- MIIDVQIBAAKCAQEA0jDs9lLWX//NXYE1kNKw4UiDVMHHEtTF1OzJvBJvUh3/xMlUic8mUpIMU5mt7BTjcijyLLl/TeNBcI/xDvWH3PAfCjP1CmNzOMHwU6wKA4Q20m5vzjauVyc
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIICVAIBAAJ/OwswbFo/uyC8ltGf/yA1A+gV5IGdnAgPbUSI3GzbHCA+x+TLG/tLvbRw3r1smppY/jkkpiVW1ErSMuN0uixp5gb78Z9rH1XpWb5WWgp3WaY/9EHMjMdOkQ/9LVZv
critical	Asymmetric Private Key	--BEGIN DSA PRIVATE KEY-- MIIBugIBAAKBgQCG9coD3P6yJQY/+DCgx2m53Z1hU62R184n94fEMni0R+ZTO4axi+1uiki3hKFMJSxb4Nv2C4bWOFvS8S+3Y+2Ic6v9P1ui4KjApZCC6sBWk15Sna98YQRniZx
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIIEjwIBAAKB/gy7mjaWgPeFdVYDZWRCA9BNiv3pPb0es27+FKY0hszLaOw47ExCtAWpDsH48TXAfyHBYwBLguayfk4LGIupxb+CGMbRo3xEp0CbfY1Jby26T9vGjRC1foHDDUJ
critical	Asymmetric Private Key	--BEGIN PRIVATE KEY-- MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAKulUTZ8B1qccZ8cDXRGSY08gW8KvLlcxxxGC4gZHNT3CBUF8n5R4KE30aZyYZ/rtsQZu05juZJxaJ0qmbe75d
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIICVAIBAAJ/OwswbFo/uyC8ltGf/yA1A+gV5IGdnAgPbUSI3GzbHCA+x+TLG/tLvbRw3r1smppY/jkkpiVW1ErSMuN0uixp5gb78Z9rH1XpWb5WWgp3WaY/9EHMjMdOkQ/9LVZv
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIIEjwIBAAKB/gy7mjaWgPeFdVYDZWRCA9BNiv3pPb0es27+FKY0hszLaOw47ExCtAWpDsH48TXAfyHBYwBLguayfk4LGIupxb+CGMbRo3xEp0CbfY1Jby26T9vGjRC1foHDDUJ
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIICXQIBAAKBgQDx3wdzpq2rvwm3Ucun1qAD/ClB+wW+RhR1nVix286QvaNqePAdCAwwLL82NqXcVQRbQ4s95splQnwvjgkFdKVXFTjPKKJI5aV3wSRN61EBVPdYpCre535yf
critical	Asymmetric Private Key	--BEGIN RSA PRIVATE KEY-- MIICXgIBAAKBgQDCFENGw33yGihy92pDjZQhl0C36rPJj+CvfSC8+q28hxA161QFNUd13wuCTUcq0Qd2qsBe/2hFyc2DCJJg0h1L78+6Z4UMR7EOcpfdUE9Hf3m/hs+FUR45uB
medium	Possible WP-config files	define ('DB_HOSTNAME', 'localhost'
low	Dominios expuestos	FROM dockerhub.hi.inet
low	Dominios expuestos	te --quiet https://artifactory.hi.inet
low	Dominios expuestos	image = "dockerhub.hi.inet
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet

low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet

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/InfolysisNetApp/wiki/secrets-Telefonica-Evolved5g-InfolysisNetApp

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/InfolysisNetApp Network apps are composed of the following services:

- infolysisnetapp

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
infolysisnetapp		
	80	OK

Publication of Network App docker images

Urls of Images published:

Image: **infolysisnetapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/infolysisnetapp:4.0
- dockerhub.hi.inet/evolved-5g/validation/infolysisnetapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:infolysisnetapp-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:infolysisnetapp-latest

USE OF 5G APIs

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

Repo used for Validation: **https://github.com//EVOLVED-5G/InfolysisNetApp**
Branch used for Validation: evolved5g
Last commit ID: 7f10808ac5d6e04630ecc1f03c12166eec21f0eb
Environment used: **kubernetes-uma**
Build number at Jenkins: 899

The individual result of the validations test is 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

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/InfolysisNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 7f10808ac5d6e04630ecc1f03c12166eec21f0eb

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
MIT License	1

Dependencies Results

Compatible	Package	Version	License
✔	sphinx_rtd_theme	1.3.0	MIT License

evolved 5G

Network App Validation Report: CafaTechNetApp4

Date: 27/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **CafaTechNetApp4** version **4.1**

Validation triggered by JORGE / jms
Repo used for Validation: **https://github.com/EVOLVED-5G/CafaTechNetApp4**
Branch used for Validation: evolved5g
Last commit ID: f07363439830d4ccd707d9be2c0a5fb9ac157e99
Environment used: **kubernetes-uma**
Build number at Jenkins: 909
Network App deploy time KPI: **19 seconds**
Total validation time: **35 Min**

The result of the Validation Process over the Network App **CafaTechNetApp4** has been: **SUCCESS**

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

Step	Step Name	Result
0	SOURCE CODE STATIC ANALYSIS	SUCCESS
1	SOURCE CODE SECURITY ANALYSIS	SUCCESS
2	SOURCE CODE SECRETS LEAKAGE	SUCCESS
3	NETWORK APP BUILD AND PORT CHECK	SUCCESS
4	IMAGE SECURITY ANALYSIS	SUCCESS
5	DEPLOY CAFATECHNETAPP4 NETWORK APP	SUCCESS
6	USE OF 5G APIS	SUCCESS
7	OPEN SOURCE LICENSES REPORT	SUCCESS

Congratulations your Network App CafaTechNetApp4 has been validated

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

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/CafaTechNetApp4
Branch used for the Analysis: evolved5g
Last Commit ID: f07363439830d4ccd707d9be2c0a5fb9ac157e99

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

Scan of cafatechnetapp4

Summary

Severity	Number of vulnerabilities
blocker	0
critical	0
major	1
minor	2

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-cafatechnetapp4-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/CafaTechNetApp4
Branch used for the Analysis: evolved5g
Last Commit ID: f07363439830d4ccd707d9be2c0a5fb9ac157e99

The security scan has been performed using Trivy version 0.35.0

Scan of repo: CafaTechNetApp4

Summary

Severity	Number of vulnerabilities
HIGH	5
MEDIUM	3
LOW	4

Good work. Network App code does not have any security issue.

The Source Code 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/CafaTechNetApp4/wiki/Telefonica-Evolved5g-CafaTechNetApp4

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/CafaTechNetApp4
Branch used for the Analysis: evolved5g
Last Commit ID: f07363439830d4ccd707d9be2c0a5fb9ac157e99

Summary

Rule	Number of secrets leaked
Dominios expuestos	18

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/iac/terraform/main.tf#L12-L12)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/pac/Jenkins-build.groovy#L43-L43)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/pac/Jenkins-build.groovy#L44-L44)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/pac/Jenkins-build.groovy#L45-L45)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/pac/Jenkins-build.groovy#L46-L46)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/iac/slave/Dockerfile#L4-L4)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/iac/slave/Dockerfile#L77-L77)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/pac/Jenkins-deploy.groovy#L13-L13)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4e5f46874063d52e095f8a7ea5c183097f01bae6/pac/Jenkins-destroy.groovy#L13-L13)	Evolved5G	2023-04-13 08:08
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 09:57
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-CafaTechNetApp4/blob/4d06cc7ad21cab69adf07ede321aac50110d7338/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 09:57

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/CafaTechNetApp4/wiki/secrets-Telefonica-Evolved5g-CafaTechNetApp4

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/CafaTechNetApp4 Network apps are composed of the following services:

- cafatechnetapp4-cafatech-netapp-4

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
cafatechnetapp4-cafatech-netapp-4		
	5555	OK

Publication of Network App docker images

Urls of Images published:

Image: **cafatechnetapp4-cafatech-netapp-4**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/cafatechnetapp4/cafatechnetapp4-cafatech-netapp-4:4.1
- dockerhub.hi.inet/evolved-5g/validation/cafatechnetapp4/cafatechnetapp4-cafatech-netapp-4:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:cafatechnetapp4-cafatech-netapp-4-4.1
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:cafatechnetapp4-cafatech-netapp-4-latest

IMAGE SECURITY ANALYSIS OF 4 1 / 1

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **4**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/CafaTechNetApp4
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	65
MEDIUM	220
LOW	496
UNKNOWN	1

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-25775 (https://nvd.nist.gov/vuln/detail/CVE-2023-25775)	Improper access control	linux-libc-dev	6.1.52-1	
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	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:9.2p1-2	

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/CafaTechNetApp4/wiki/dockerhub.hi.inet-evolved-5g-validation-cafatechnetapp4-cafatechnetapp4-cafatech-netapp-4

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **CafaTechNetApp4** version **4.1**

Repo used for Validation: **https://github.com/EVOLVED-5G/CafaTechNetApp4**
Branch used for Validation: evolved5g
Last commit ID: f07363439830d4ccd707d9be2c0a5fb9ac157e99
Environment used: **kubernetes-uma**
Build number at Jenkins: 909

The individual result of the validations test is 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

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/CafaTechNetApp4
Branch used for the Analysis: evolved5g
Last Commit ID: f07363439830d4ccd707d9be2c0a5fb9ac157e99

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	11
MIT License	20
GNU Library or Lesser General Public License (LGPL)	2
Apache Software License	7
Mozilla Public License 2.0 (MPL 2.0)	1
Apache Software License;; BSD License	2
BSD License;; Apache Software License	1
Artistic License;; GNU General Public License (GPL);; GNU General Public License v2 or later (GPLv2+)	1
Python Software Foundation License	1

Dependencies Results

Compatible	Package	Version	License
✔	Click	7.0	BSD License
✔	Jinja2	2.10.1	BSD License
✔	MarkupSafe	1.1.0	BSD License
✔	PyYAML	6.0	MIT License
✔	argh	0.29.4	GNU Library or Lesser General Public License (LGPL)
✔	arrow	1.2.3	Apache Software License
✔	attrs	21.4.0	MIT License
✔	binaryornot	0.4.4	BSD License
✔	certifi	2019.11.28	Mozilla Public License 2.0 (MPL 2.0)
✔	cffi	1.15.1	MIT License
✔	chardet	3.0.4	GNU Library or Lesser General Public License (LGPL)
✔	charset-normalizer	3.1.0	MIT License
✔	cookiecutter	2.3.1	BSD License
✔	coverage	7.3.1	Apache Software License
✔	cryptography	2.8	Apache Software License;; BSD License
✔	evolved5g	1.0.13	Apache Software License
✔	flake8	6.1.0	MIT License
✔	flask	2.3.3	BSD License
✔	flask-cors	4.0.0	MIT License
✔	idna	2.8	BSD License
✔	importlib-metadata	1.5.0	Apache Software License
✔	iniconfig	2.0.0	MIT License
✔	invoke	2.2.0	BSD License
✔	itsdangerous	2.1.2	BSD License
✔	jinja2-time	0.2.0	MIT License

✔	mccabe	0.7.0	MIT License
✔	packaging	23.0	Apache Software License;; BSD License
✔	pathtools	0.1.2	MIT License
✔	pluggy	1.3.0	MIT License
✔	py	1.11.0	MIT License
✔	pyOpenSSL	19.0.0	Apache Software License
✔	pycodestyle	2.11.0	MIT License
✔	pycparser	2.21	BSD License
✔	pyflakes	3.1.0	MIT License
✔	pytest	7.4.2	MIT License
✔	python-dateutil	2.8.2	BSD License;; Apache Software License
✔	python-slugify	8.0.1	MIT License
✔	requests	2.31.0	Apache Software License
✔	six	1.14.0	MIT License
	text-unidecode	1.3	Artistic License;; GNU General Public License (GPL);; GNU General Public License v2 or later (GPLv2+)
✔	toml	0.10.2	MIT License
✔	typing_extensions	4.7.1	Python Software Foundation License
✔	urllib3	1.26.15	MIT License
✔	watchdog	3.0.0	Apache Software License
✔	werkzeug	2.3.7	BSD License
✔	zipp	1.0.0	MIT License

evolved 5G

Network App Validation Report: ZortenetNetApp

Date: 26/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **ZortenetNetApp** version **4.0**

Validation triggered by JORGE / jms
Repo used for Validation: **https://github.com/EVOLVED-5G/ZortenetNetApp**
Branch used for Validation: evolved5g
Last commit ID: e8ec2ac4817d958808c21f325991528cbfe1ce43
Environment used: **kubernetes-uma**
Build number at Jenkins: 897
Network App deploy time KPI: **17 seconds**
Total validation time: **35 Min**

The result of the Validation Process over the Network App **ZortenetNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App ZortenetNetApp has been validated

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

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/ZortenetNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e8ec2ac4817d958808c21f325991528cbfe1ce43

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

Scan of zortenetnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	3
major	9
minor	12

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-zortenetnetapp-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/ZortenetNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e8ec2ac4817d958808c21f325991528cbfe1ce43

The security scan has been performed using Trivy version 0.35.0

Scan of repo: ZortenetNetApp

Summary

Severity	Number of vulnerabilities
MEDIUM	1

Good work. Network App code does not have any security issue.

The Source Code 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/ZortenetNetApp/wiki/Telefonica-Evolved5g-ZortenetNetApp

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/ZortenetNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e8ec2ac4817d958808c21f325991528cbfe1ce43

Summary

Rule	Number of secrets leaked
Dominios expuestos	9

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-09-19 10:51
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-ZortenetNetApp/blob/02b2c5816f581e8957991f6bbe8b73c744b2d2d2/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-09-19 10:51

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/ZortenetNetApp/wiki/secrets-Telefonica-Evolved5g-ZortenetNetApp

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/ZortenetNetApp Network apps are composed of the following services:

- zortenetnetapp-zorte_netapp
- zortenetnetapp-grafana
- zortenetnetapp-influxdb

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
zortenetnetapp-zorte_netapp		
	5000	OK
zortenetnetapp-grafana		
	3000	OK
zortenetnetapp-influxdb		
	8086	OK

Publication of Network App docker images

Urls of Images published:

Image: **zortenetnetapp-zorte_netapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/zortenetnetapp/zortenetnetapp-zorte_netapp:4.0
- dockerhub.hi.inet/evolved-5g/validation/zortenetnetapp/zortenetnetapp-zorte_netapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:zortenetnetapp-zorte_netapp-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:zortenetnetapp-zorte_netapp-latest

Image: **zortenetnetapp-grafana**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/zortenetnetapp/zortenetnetapp-grafana:4.0
- dockerhub.hi.inet/evolved-5g/validation/zortenetnetapp/zortenetnetapp-grafana:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:zortenetnetapp-grafana-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:zortenetnetapp-grafana-latest

Image: **zortenetnetapp-influxdb**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/zortenetnetapp/zortenetnetapp-influxdb:4.0
- dockerhub.hi.inet/evolved-5g/validation/zortenetnetapp/zortenetnetapp-influxdb:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:zortenetnetapp-influxdb-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:zortenetnetapp-influxdb-latest

IMAGE SECURITY ANALYSIS OF grafana 1 / 3

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

Summary

Severity	Number of vulnerabilities
CRITICAL	1
HIGH	27
MEDIUM	178
LOW	97

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2022-41912 (https://nvd.nist.gov/vuln/detail/CVE-2022-41912)	Authentication bypass when processing SAML responses containing multiple Assertion elements	github.com/crewjam/saml	v0.4.6-0.20201227203850-bca570abb2ce	0.4.9

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/ZortenetNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-zortenetnetapp-zortenetnetapp-grafana

IMAGE SECURITY ANALYSIS OF influxdb 2 / 3

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

Good work. No vulnerabilities found.

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/ZortenetNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-zortenetnetapp-zortenetnetapp-influxdb

IMAGE SECURITY ANALYSIS OF zorte_netapp 3 / 3

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

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	61
MEDIUM	219
LOW	494
UNKNOWN	1

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-25775 (https://nvd.nist.gov/vuln/detail/CVE-2023-25775)	Improper access control	linux-libc-dev	6.1.52-1	
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	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:9.2p1-2	

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/ZortenetNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-zortenetnetapp-zortenetnetapp-zorte_netapp

USE OF 5G APIs

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

Repo used for Validation: **https://github.com/EVOLVED-5G/ZortenetNetApp**
Branch used for Validation: evolved5g
Last commit ID: e8ec2ac4817d958808c21f325991528cbfe1ce43
Environment used: **kubernetes-uma**
Build number at Jenkins: 897

The individual result of the validations test is 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-monitoring-event/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

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/ZortenetNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: e8ec2ac4817d958808c21f325991528cbfe1ce43

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
MIT License	3
Apache Software License	3
BSD License	1

Dependencies Results

Compatible	Package	Version	License
✔	PyJWT	1.7.1	MIT License
✔	evolved5g	1.0.13	Apache Software License
✔	flask	2.3.3	BSD License
✔	flask-cors	4.0.0	MIT License
✔	influxdb	5.3.1	MIT License
✔	pyOpenSSL	19.0.0	Apache Software License
✔	requests	2.31.0	Apache Software License

evolved 5G

Network App Validation Report: IninRmonNetApp

Date: 28/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **IninRmonNetApp** version **4.1**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/IninRmonNetApp**
Branch used for Validation: evolved5g
Last commit ID: c2a429f70539445f13959eb23cac7a615dc486a5
Environment used: **kubernetes-uma**
Build number at Jenkins: 929
Network App deploy time KPI: **89 seconds**
Total validation time: **26 Min**

The result of the Validation Process over the Network App **IninRmonNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App IninRmonNetApp has been validated

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

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/IninRmonNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c2a429f70539445f13959eb23cac7a615dc486a5

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

Scan of ininrmonnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	26
major	12
minor	66

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-ininrmonnetapp-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/IninRmonNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c2a429f70539445f13959eb23cac7a615dc486a5

The security scan has been performed using Trivy version 0.35.0

Scan of repo: IninRmonNetApp

Summary

Severity	Number of vulnerabilities
MEDIUM	2

Good work. Network App code does not have any security issue.

The Source Code 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/IninRmonNetApp/wiki/Telefonica-Evolved5g-IninRmonNetApp

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/IninRmonNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c2a429f70539445f13959eb23cac7a615dc486a5

Summary

Rule	Number of secrets leaked
Dominios expuestos	9

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/iac/terraform/main.tf#L12-L12)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/iac/slave/Dockerfile#L4-L4)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/iac/slave/Dockerfile#L77-L77)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/pac/Jenkins-build.groovy#L43-L43)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/pac/Jenkins-build.groovy#L44-L44)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/pac/Jenkins-build.groovy#L45-L45)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/pac/Jenkins-build.groovy#L46-L46)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/pac/Jenkins-deploy.groovy#L13-L13)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-IninRmonNetApp/blob/e065e68a8b0d0601b53fa7563838a711f12163b8/pac/Jenkins-destroy.groovy#L13-L13)	ALEJANDRO MOLINA SANCHEZ	2022-05-24 13:55

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/IninRmonNetApp/wiki/secrets-Telefonica-Evolved5g-IninRmonNetApp

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/IninRmonNetApp Network apps are composed of the following services:

- ininrmonnetapp-rmonnetapp
- ininrmonnetapp-ininrmonnetapp_rmonnetapp_1

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
ininrmonnetapp-rmonnetapp		
	80	OK
ininrmonnetapp-ininrmonnetapp_rmonnetapp_1		

Publication of Network App docker images

Urls of Images published:

Image: **ininrmonnetapp-rmonnetapp**

Evolved-5G open repository:

Evolved-5G AWS Docker Registry:

Image: **ininrmonnetapp-ininrmonnetapp_rmonnetapp_1**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/ininrmonnetapp/ininrmonnetapp-ininrmonnetapp_rmonnetapp_1:4.1
- dockerhub.hi.inet/evolved-5g/validation/ininrmonnetapp/ininrmonnetapp-ininrmonnetapp_rmonnetapp_1:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:ininrmonnetapp-ininrmonnetapp_rmonnetapp_1-4.1
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:ininrmonnetapp-ininrmonnetapp_rmonnetapp_1-latest

IMAGE SECURITY ANALYSIS OF ininrmonnetapp_rmonnetapp_1 1 / 1

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **ininrmonnetapp_rmonnetapp_1**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/IninRmonNetApp
Branch used for the Analysis: evolved5g

Good work. No vulnerabilities found.

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/IninRmonNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-ininrmonnetapp-ininrmonnetapp-ininrmonnetapp_rmonnetapp_1

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **IninRmonNetApp** version **4.1**

Repo used for Validation: **https://github.com/EVOLVED-5G/IninRmonNetApp**
Branch used for Validation: evolved5g
Last commit ID: c2a429f70539445f13959eb23cac7a615dc486a5
Environment used: **kubernetes-uma**
Build number at Jenkins: 929

The individual result of the validations test is 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

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/IninRmonNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c2a429f70539445f13959eb23cac7a615dc486a5

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	1
Apache Software License	3
MIT License	2

Dependencies Results

Compatible	Package	Version	License
✔	MarkupSafe	1.1.0	BSD License
✔	aiohttp	3.8.5	Apache Software License
✔	dataclasses	0.8	Apache Software License
✔	pytz	2023.3.post1	MIT License
✔	requests	2.31.0	Apache Software License
✔	setuptools-rust	1.7.0	MIT License

evolved
5G

Network App Validation Report: UmaCsicNetApp

Date: 26/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **UmaCsicNetApp** version **1.0.13**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/UmaCsicNetApp**
Branch used for Validation: evolved5g
Last commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d
Environment used: **kubernetes-uma**
Build number at Jenkins: 896
Network App deploy time KPI: **4 seconds**
Total validation time: **31 Min**

The result of the Validation Process over the Network App **UmaCsicNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App UmaCsicNetApp has been validated

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

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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

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

Scan of umacsicnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	3
major	1
minor	1

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-umacsicnetapp-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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

The security scan has been performed using Trivy version 0.35.0

Scan of repo: UmaCsicNetApp

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/UmaCsicNetApp/wiki/Telefonica-Evolved5g-UmaCsicNetApp

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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

Summary

Rule	Number of secrets leaked
Dominios expuestos	4

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	ttp://umacsic-nef.apps.ocp-epg.hi.inet	k8s/netapp/environment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/environment.yaml#L12-L12)	Evolved5G	2023-09-26 09:31
low	Dominios expuestos	T: "umacsic-capif.apps.ocp-epg.hi.inet	k8s/netapp/environment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/environment.yaml#L15-L15)	Evolved5G	2023-09-26 09:31
low	Dominios expuestos	- umacsic-nef.apps.ocp-epg.hi.inet	k8s/netapp/deployment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/deployment.yaml#L124-L124)	Evolved5G	2023-09-26 09:31
low	Dominios expuestos	- umacsic-capif.apps.ocp-epg.hi.inet	k8s/netapp/deployment.yaml (https://github.com/Telefonica/Evolved5g-UmaCsicNetApp/blob/84b1430df18a3bdd04699c33724fadaae45ee896/k8s/netapp/deployment.yaml#L125-L125)	Evolved5G	2023-09-26 09:31

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/UmaCsicNetApp/wiki/secrets-Telefonica-Evolved5g-UmaCsicNetApp

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/UmaCsicNetApp Network apps are composed of the following services:

- umacsicnetapp-netapp

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
umacsicnetapp-netapp		
	10001	OK

Publication of Network App docker images

Urls of Images published:

Image: **umacsicnetapp-netapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/umacsicnetapp/umacsicnetapp-netapp:1.0.13
- dockerhub.hi.inet/evolved-5g/validation/umacsicnetapp/umacsicnetapp-netapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:umacsicnetapp-netapp-1.0.13
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:umacsicnetapp-netapp-latest

IMAGE SECURITY ANALYSIS OF netapp 1 / 2

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

Summary

Severity	Number of vulnerabilities
HIGH	6
MEDIUM	20
LOW	62

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion

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/UmaCsicNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-umacsicnetapp-umacsicnetapp-netapp

IMAGE SECURITY ANALYSIS OF postgres_container 2 / 2

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

Summary

Severity	Number of vulnerabilities
HIGH	10
MEDIUM	22
LOW	103

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion

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/UmaCsicNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-umacsicnetapp-umacsicnetapp-postgres_container

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **UmaCsicNetApp** version **1.0.13**

Repo used for Validation: **https://github.com/EVOLVED-5G/UmaCsicNetApp**
Branch used for Validation: evolved5g
Last commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d
Environment used: **kubernetes-uma**
Build number at Jenkins: 896

The individual result of the validations test is 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-monitoring-event/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

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/UmaCsicNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: ba0400a39011a2ba2296c2138e6dc8edb558087d

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
Apache Software License	2
BSD License	4
MIT License	4
GNU Library or Lesser General Public License (LGPL)	1
Zope Public License	1

Dependencies Results

Compatible	Package	Version	License
✔	evolved5g	1.0.13	Apache Software License
✔	flask	2.3.3	BSD License
✔	flask-cors	4.0.0	MIT License
✔	flask_marshmallow	0.15.0	MIT License
✔	flask_migrate	4.0.5	MIT License
✔	flask_restful	0.3.10	BSD License
✔	flask_sqlalchemy	3.1.1	BSD License
✔	marshmallow-sqlalchemy	0.29.0	MIT License
✔	psycopg2-binary	2.9.7	GNU Library or Lesser General Public License (LGPL)
✔	python-dotenv	1.0.0	BSD License
✔	requests	2.31.0	Apache Software License
	waitress	2.1.2	Zope Public License

evolved 5G

Network App Validation Report: 8BellsNetApp

Date: 29/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **8BellsNetApp** version **4.0**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/8BellsNetApp**
Branch used for Validation: evolved5g
Last commit ID: be206acc4f4031f5c02f21cad7fcc40b4b46f226
Environment used: **kubernetes-uma**
Build number at Jenkins: 938
Network App deploy time KPI: **26 seconds**
Total validation time: **40 Min**

The result of the Validation Process over the Network App **8BellsNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App 8BellsNetApp has been validated

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

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/8BellsNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: be206acc4f4031f5c02f21cad7fcc40b4b46f226

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

Scan of 8bellsnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	21
major	33
minor	12

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-8bellsnetapp-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/8BellsNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: be206acc4f4031f5c02f21cad7fcc40b4b46f226

The security scan has been performed using Trivy version 0.35.0

Scan of repo: 8BellsNetApp

Summary

Severity	Number of vulnerabilities
MEDIUM	1

Good work. Network App code does not have any security issue.

The Source Code 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/8BellsNetApp/wiki/Telefonica-Evolved5g-8BellsNetApp

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/8BellsNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: be206acc4f4031f5c02f21cad7fcc40b4b46f226

Summary

Rule	Number of secrets leaked
Asymmetric Private Key	2
Dominios expuestos	27

Passwords detected in commit history

Severity	Description	Match
low	Dominios expuestos	image = "dockerhub.hi.inet
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet
low	Dominios expuestos	FROM dockerhub.hi.inet
low	Dominios expuestos	te --quiet https://artifactory.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet
low	Dominios expuestos	image = "dockerhub.hi.inet
low	Dominios expuestos	FROM dockerhub.hi.inet
low	Dominios expuestos	te --quiet https://artifactory.hi.inet
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet
critical	Asymmetric Private Key	--BEGIN PRIVATE KEY-- MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDTvKGu7qe7Aqx0qtzW0Qa4x7phVNwmpI9JigRiSO3ajkbNso8a8Ex+WlkPA2VNEXBKyzfIGeCORUJqKAs+nB
low	Dominios expuestos	image = "dockerhub.hi.inet
low	Dominios expuestos	FROM dockerhub.hi.inet
low	Dominios expuestos	te --quiet https://artifactory.hi.inet
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet

low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet
critical	Asymmetric Private Key	--BEGIN PRIVATE KEY-- MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDTvKGu7qe7Aqx0qtzW0Qa4x7phVNwmpI9JigRiSO3ajkbNso8a8Ex+WlkPA2VNEXBKyzfIGeCORUJqKAs+nB

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/8BellsNetApp/wiki/secrets-Telefonica-Evolved5g-8BellsNetApp

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/8BellsNetApp Network apps are composed of the following services:

- 8bellsnetapp-8b_netapp
- 8bellsnetapp-8b_netapp_db
- 8bellsnetapp-8b_netapp_adminer

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
8bellsnetapp-8b_netapp		
	5000	OK
8bellsnetapp-8b_netapp_db		
	5432	OK
8bellsnetapp-8b_netapp_adminer		
	8008	OK

Publication of Network App docker images

Urls of Images published:

Image: **8bellsnetapp-8b_netapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/8bellsnetapp/8bellsnetapp-8b_netapp:4.0
- dockerhub.hi.inet/evolved-5g/validation/8bellsnetapp/8bellsnetapp-8b_netapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:8bellsnetapp-8b_netapp-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:8bellsnetapp-8b_netapp-latest

Image: **8bellsnetapp-8b_netapp_db**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/8bellsnetapp/8bellsnetapp-8b_netapp_db:4.0
- dockerhub.hi.inet/evolved-5g/validation/8bellsnetapp/8bellsnetapp-8b_netapp_db:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:8bellsnetapp-8b_netapp_db-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:8bellsnetapp-8b_netapp_db-latest

Image: **8bellsnetapp-8b_netapp_adminer**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/8bellsnetapp/8bellsnetapp-8b_netapp_adminer:4.0
- dockerhub.hi.inet/evolved-5g/validation/8bellsnetapp/8bellsnetapp-8b_netapp_adminer:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:8bellsnetapp-8b_netapp_adminer-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:8bellsnetapp-8b_netapp_adminer-latest

IMAGE SECURITY ANALYSIS OF 8b_netapp 1 / 3

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **8b_netapp**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/8BellsNetApp
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
CRITICAL	85
HIGH	865
MEDIUM	1216
LOW	1437
UNKNOWN	37

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-2022-1664 (https://nvd.nist.gov/vuln/detail/CVE-2022-1664)	Dpkg::Source::Archive in dpkg, the Debian package management system, b ...	dpkg	1.19.7	1.19.8
CRITICAL	CVE-2022-1664 (https://nvd.nist.gov/vuln/detail/CVE-2022-1664)	Dpkg::Source::Archive in dpkg, the Debian package management system, b ...	dpkg-dev	1.19.7	1.19.8
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-2021-43400 (https://nvd.nist.gov/vuln/detail/CVE-2021-43400)	bluez: use-after-free in gatt-database.c	libbluetooth-dev	5.50-1.2~deb10u1	5.50-1.2~deb10u3
CRITICAL	CVE-2021-43400 (https://nvd.nist.gov/vuln/detail/CVE-2021-43400)	bluez: use-after-free in gatt-database.c	libbluetooth3	5.50-1.2~deb10u1	5.50-1.2~deb10u3
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	2.28-10+deb10u2
	CVE-2022-32221		libcurl3-		7.64.0-

CRITICAL	(https://nvd.nist.gov/vuln/detail/CVE-2022-32221)	POST following PUT confusion	gnutls	7.64.0-4+deb10u2	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	
CRITICAL	CVE-2019-8457 (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-2022-1664 (https://nvd.nist.gov/vuln/detail/CVE-2022-1664)	Dpkg::Source::Archive in dpkg, the Debian package management system, b ...	libdpkg-perl	1.19.7	1.19.8
CRITICAL	CVE-2022-22822 (https://nvd.nist.gov/vuln/detail/CVE-2022-22822)	Integer overflow in addBinding in xmlparse.c	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-22823 (https://nvd.nist.gov/vuln/detail/CVE-2022-22823)	Integer overflow in build_model in xmlparse.c	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-22824 (https://nvd.nist.gov/vuln/detail/CVE-2022-22824)	Integer overflow in defineAttribute in xmlparse.c	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-23852 (https://nvd.nist.gov/vuln/detail/CVE-2022-23852)	Integer overflow in function XML_GetBuffer	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-25235 (https://nvd.nist.gov/vuln/detail/CVE-2022-25235)	Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u3
CRITICAL	CVE-2022-25236 (https://nvd.nist.gov/vuln/detail/CVE-2022-25236)	prefix]" attribute values can lead to arbitrary code execution	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u3
CRITICAL	CVE-2022-25315 (https://nvd.nist.gov/vuln/detail/CVE-2022-25315)	Integer overflow in storeRawNames()	libexpat1	2.2.6-2+deb10u1	2.2.6-2+deb10u3
CRITICAL	CVE-2022-22822 (https://nvd.nist.gov/vuln/detail/CVE-2022-22822)	Integer overflow in addBinding in xmlparse.c	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-22823 (https://nvd.nist.gov/vuln/detail/CVE-2022-22823)	Integer overflow in build_model in xmlparse.c	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-22824 (https://nvd.nist.gov/vuln/detail/CVE-2022-22824)	Integer overflow in defineAttribute in xmlparse.c	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-23852 (https://nvd.nist.gov/vuln/detail/CVE-2022-23852)	Integer overflow in function XML_GetBuffer	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u2
CRITICAL	CVE-2022-25235 (https://nvd.nist.gov/vuln/detail/CVE-2022-25235)	Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u3
CRITICAL	CVE-2022-25236 (https://nvd.nist.gov/vuln/detail/CVE-2022-25236)	prefix]" attribute values can lead to arbitrary code execution	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u3
CRITICAL	CVE-2022-25315 (https://nvd.nist.gov/vuln/detail/CVE-2022-25315)	Integer overflow in storeRawNames()	libexpat1-dev	2.2.6-2+deb10u1	2.2.6-2+deb10u3
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)	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)	integer overflow to code execution	libksba8	1.3.5-2	1.3.5-2+deb10u2
CRITICAL	CVE-2022-29155 (https://nvd.nist.gov/vuln/detail/CVE-2022-29155)	OpenLDAP SQL injection	libldap-2.4-2	2.4.47+dfsg-3+deb10u6	2.4.47+dfsg-3+deb10u7
CRITICAL	CVE-2022-29155 (https://nvd.nist.gov/vuln/detail/CVE-2022-29155)	OpenLDAP SQL injection	libldap-common	2.4.47+dfsg-3+deb10u6	2.4.47+dfsg-3+deb10u7
CRITICAL	CVE-2022-1586 (https://nvd.nist.gov/vuln/detail/CVE-2022-1586)	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)	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)	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)	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)	XML External Entity in XML processing plistlib module	libpython3.7-minimal	3.7.3-2+deb10u3	
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	libpython3.7-stdlib	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	XML External Entity in XML processing plistlib module	libpython3.7-stdlib	3.7.3-2+deb10u3	

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-2021-3711 (https://nvd.nist.gov/vuln/detail/CVE-2021-3711)	SM2 Decryption Buffer Overflow	libssl-dev	1.1.1d-0+deb10u6	1.1.1d-0+deb10u7
CRITICAL	CVE-2022-1292 (https://nvd.nist.gov/vuln/detail/CVE-2022-1292)	c_rehash script allows command injection	libssl-dev	1.1.1d-0+deb10u6	1.1.1n-0+deb10u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	libssl-dev	1.1.1d-0+deb10u6	1.1.1n-0+deb10u3
CRITICAL	CVE-2021-3711 (https://nvd.nist.gov/vuln/detail/CVE-2021-3711)	SM2 Decryption Buffer Overflow	libssl1.1	1.1.1d-0+deb10u6	1.1.1d-0+deb10u7
CRITICAL	CVE-2022-1292 (https://nvd.nist.gov/vuln/detail/CVE-2022-1292)	c_rehash script allows command injection	libssl1.1	1.1.1d-0+deb10u6	1.1.1n-0+deb10u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	libssl1.1	1.1.1d-0+deb10u6	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-2023-38408 (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-2021-3711 (https://nvd.nist.gov/vuln/detail/CVE-2021-3711)	SM2 Decryption Buffer Overflow	openssl	1.1.1d-0+deb10u6	1.1.1d-0+deb10u7
CRITICAL	CVE-2022-1292 (https://nvd.nist.gov/vuln/detail/CVE-2022-1292)	c_rehash script allows command injection	openssl	1.1.1d-0+deb10u6	1.1.1n-0+deb10u2
CRITICAL	CVE-2022-2068 (https://nvd.nist.gov/vuln/detail/CVE-2022-2068)	the c_rehash script allows command injection	openssl	1.1.1d-0+deb10u6	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)	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)	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)	XML External Entity in XML processing plistlib module	python3.7	3.7.3-2+deb10u3	
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	python3.7-minimal	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	XML External Entity in XML processing plistlib module	python3.7-minimal	3.7.3-2+deb10u3	
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	1:1.2.11.dfsg-1+deb10u2
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	1:1.2.11.dfsg-1+deb10u2

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/8BellsNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-8bellsnetapp-8bellsnetapp-8b_netapp

IMAGE SECURITY ANALYSIS OF 8b_netapp_adminer 2 / 3

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **8b_netapp_adminer**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/8BellsNetApp
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
CRITICAL	9
HIGH	78
MEDIUM	45
LOW	12

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2021-36159 (https://nvd.nist.gov/vuln/detail/CVE-2021-36159)	an out of boundary read while libfetch uses strtol to parse the relevant numbers into address bytes	apk-tools	2.12.1-r0	2.12.6-r0
CRITICAL	CVE-2021-22945 (https://nvd.nist.gov/vuln/detail/CVE-2021-22945)	curl: use-after-free and double-free in MQTT sending	curl	7.74.0-r0	7.79.0-r0
CRITICAL	CVE-2022-32207 (https://nvd.nist.gov/vuln/detail/CVE-2022-32207)	Unpreserved file permissions	curl	7.74.0-r0	7.79.1-r2
CRITICAL	CVE-2021-3711 (https://nvd.nist.gov/vuln/detail/CVE-2021-3711)	SM2 Decryption Buffer Overflow	libcrypto1.1	1.1.1i-r0	1.1.1l-r0
CRITICAL	CVE-2021-22945 (https://nvd.nist.gov/vuln/detail/CVE-2021-22945)	curl: use-after-free and double-free in MQTT sending	libcurl	7.74.0-r0	7.79.0-r0
CRITICAL	CVE-2022-32207 (https://nvd.nist.gov/vuln/detail/CVE-2022-32207)	Unpreserved file permissions	libcurl	7.74.0-r0	7.79.1-r2
CRITICAL	CVE-2021-3711 (https://nvd.nist.gov/vuln/detail/CVE-2021-3711)	SM2 Decryption Buffer Overflow	libssl1.1	1.1.1i-r0	1.1.1l-r0
CRITICAL	CVE-2021-3711 (https://nvd.nist.gov/vuln/detail/CVE-2021-3711)	SM2 Decryption Buffer Overflow	openssl	1.1.1i-r0	1.1.1l-r0
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	zlib	1.2.11-r3	1.2.12-r2

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/8BellsNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-8bellsnetapp-8bellsnetapp-8b_netapp_adminer

IMAGE SECURITY ANALYSIS OF 8b_netapp_db 3 / 3

Test Description: This test detects vulnerabilities in the Network App docker images built.
Network App image under study: **8b_netapp_db**
Network App repository used for the analysis: https://github.com/EVOLVED-5G/8BellsNetApp
Branch used for the Analysis: evolved5g

Summary

Severity	Number of vulnerabilities
HIGH	6
MEDIUM	26
LOW	103

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion

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/8BellsNetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-8bellsnetapp-8bellsnetapp-8b_netapp_db

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **8BellsNetApp** version **4.0**

Repo used for Validation: **https://github.com/EVOLVED-5G/8BellsNetApp**
Branch used for Validation: evolved5g
Last commit ID: be206acc4f4031f5c02f21cad7fcc40b4b46f226
Environment used: **kubernetes-uma**
Build number at Jenkins: 938

The individual result of the validations test is 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-monitoring-event/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

evolved 5G

Network App Validation Report: FogusNetApp

Date: 29/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

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

Validation triggered by JORGE / jms
Repo used for Validation: **https://github.com/EVOLVED-5G/FogusNetApp**
Branch used for Validation: evolved5g
Last commit ID: d2885d0ec48c9b78f165753242612f7557c08df6
Environment used: **kubernetes-athens**
Build number at Jenkins: 935
Network App deploy time KPI: **48 seconds**
Total validation time: **50 Min**

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

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

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

Congratulations your Network App FogusNetApp has been validated

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

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
Dominios expuestos	12

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	- 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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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	Dominios expuestos	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/validation/fogusnetapp/fogusnetapp-netappdjango:4.0
- dockerhub.hi.inet/evolved-5g/validation/fogusnetapp/fogusnetapp-netappdjango:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:fogusnetapp-netappdjango-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:fogusnetapp-netappdjango-latest

Image: **fogusnetapp-netappfe**

Evolved-5G open repository:

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

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:fogusnetapp-netappfe-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:fogusnetapp-netappfe-latest

Image: **fogusnetapp-netapppostgres**

Evolved-5G open repository:

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

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:fogusnetapp-netapppostgres-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation: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	59
MEDIUM	225
LOW	494

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-25775 (https://nvd.nist.gov/vuln/detail/CVE-2023-25775)	Improper access control	linux-libc-dev	6.1.52-1	
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	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:9.2p1-2	

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-validation-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	58
HIGH	718
MEDIUM	1013
LOW	1395
UNKNOWN	35

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)	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)	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)	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)	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)	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)	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)	XML External Entity in XML processing plistlib module	libpython3.7-minimal	3.7.3-2+deb10u3	
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	libpython3.7-stdlib	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	XML External Entity in XML processing plistlib module	libpython3.7-stdlib	3.7.3-2+deb10u3	
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-2023-38408 (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)	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)	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)	XML External Entity in XML processing plistlib module	python3.7	3.7.3-2+deb10u3	
CRITICAL	CVE-2022-37454 (https://nvd.nist.gov/vuln/detail/CVE-2022-37454)	buffer overflow in the SHA-3 reference implementation	python3.7-minimal	3.7.3-2+deb10u3	3.7.3-2+deb10u4
CRITICAL	CVE-2022-48565 (https://nvd.nist.gov/vuln/detail/CVE-2022-48565)	XML External Entity in XML processing plistlib module	python3.7-minimal	3.7.3-2+deb10u3	
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-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

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-validation-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-validation-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-athens**
Build number at Jenkins: 935

The individual result of the validations test is 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

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
MIT License	5
BSD License	5
Apache Software License	2
GNU Lesser General Public License v2 or later (LGPLv2+)	1
GNU Library or Lesser General Public License (LGPL)	1

Dependencies Results

Compatible	Package	Version	License
✔	PyJWT	1.7.1	MIT License
✔	asgiref	3.7.2	BSD License
✔	configparser	6.0.0	MIT License
✔	django	4.2.5	BSD License
✔	django-cors-headers	4.2.0	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
✔	mariadb	1.1.7	GNU Lesser General Public License v2 or later (LGPLv2+)
✔	psycopg2	2.9.8	GNU Library or Lesser General Public License (LGPL)
✔	pytz	2023.3.post1	MIT License
✔	requests	2.31.0	Apache Software License
✔	sqlparse	0.4.4	BSD License

evolved 5G

Network App Validation Report: IQB-NetApp

Date: 27/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **IQB-NetApp** version **4.0**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/IQB-NetApp**
Branch used for Validation: evolved5g
Last commit ID: 9ede78aa0e55e85456146733b2b67e59abc5a161
Environment used: **kubernetes-uma**
Build number at Jenkins: 912
Network App deploy time KPI: **21 seconds**
Total validation time: **39 Min**

The result of the Validation Process over the Network App **IQB-NetApp** has been: **SUCCESS**

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

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

Congratulations your Network App IQB-NetApp has been validated

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

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/IQB-NetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 9ede78aa0e55e85456146733b2b67e59abc5a161

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

Scan of iqb

Summary

Severity	Number of vulnerabilities
blocker	0
critical	8
major	16
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-iqb-netapp-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/IQB-NetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 9ede78aa0e55e85456146733b2b67e59abc5a161

The security scan has been performed using Trivy version 0.35.0

Scan of repo: IQB-NetApp

Summary

Severity	Number of vulnerabilities
HIGH	2
MEDIUM	1
LOW	1

Good work. Network App code does not have any security issue.

The Source Code 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/IQB-NetApp/wiki/Telefonica-Evolved5g-IQB-NetApp

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/IQB-NetApp
Branch used for the Analysis: evolved5g
Last Commit ID: 9ede78aa0e55e85456146733b2b67e59abc5a161

Summary

Rule	Number of secrets leaked
Dominios expuestos	9

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 10:46
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-IQB-NetApp/blob/577bd8e095d4414da0500432ba3cd36e331f4356/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 10:46

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/IQB-NetApp/wiki/secrets-Telefonica-Evolved5g-IQB-NetApp

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/IQB-NetApp Network apps are composed of the following services:

- iqb-netapp-keycloak
- iqb-netapp-iqb_netapp
- iqb-netapp-callbacks

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
iqb-netapp-keycloak		
	8980	OK
iqb-netapp-iqb_netapp		
	5000	OK
iqb-netapp-callbacks		
	5002	OK

Publication of Network App docker images

Urls of Images published:

Image: **iqb-netapp-keycloak**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/iqb-netapp/iqb-netapp-keycloak:4.0
- dockerhub.hi.inet/evolved-5g/validation/iqb-netapp/iqb-netapp-keycloak:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:iqb-netapp-keycloak-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:iqb-netapp-keycloak-latest

Image: **iqb-netapp-iqb_netapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/iqb-netapp/iqb-netapp-iqb_netapp:4.0
- dockerhub.hi.inet/evolved-5g/validation/iqb-netapp/iqb-netapp-iqb_netapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:iqb-netapp-iqb_netapp-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:iqb-netapp-iqb_netapp-latest

Image: **iqb-netapp-callbacks**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/iqb-netapp/iqb-netapp-callbacks:4.0
- dockerhub.hi.inet/evolved-5g/validation/iqb-netapp/iqb-netapp-callbacks:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:iqb-netapp-callbacks-4.0
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:iqb-netapp-callbacks-latest

IMAGE SECURITY ANALYSIS OF callbacks 1 / 3

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

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	59
MEDIUM	217
LOW	491
UNKNOWN	1

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-25775 (https://nvd.nist.gov/vuln/detail/CVE-2023-25775)	Improper access control	linux-libc-dev	6.1.52-1	
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	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:9.2p1-2	

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/IQB-NetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-iqb-netapp-iqb-netapp-callbacks

IMAGE SECURITY ANALYSIS OF iqb_netapp 2 / 3

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

Summary

Severity	Number of vulnerabilities
CRITICAL	3
HIGH	64
MEDIUM	220
LOW	495
UNKNOWN	1

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2023-25775 (https://nvd.nist.gov/vuln/detail/CVE-2023-25775)	Improper access control	linux-libc-dev	6.1.52-1	
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	
CRITICAL	CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)	Remote code execution in ssh-agent PKCS#11 support	openssh-client	1:9.2p1-2	

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/IQB-NetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-iqb-netapp-iqb-netapp-iqb_netapp

IMAGE SECURITY ANALYSIS OF keycloak 3 / 3

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

Summary

Severity	Number of vulnerabilities
CRITICAL	19
HIGH	82
MEDIUM	287
LOW	90
UNKNOWN	1

Critical Vulnerabilities

Severity	ID	Title	PkgName	InstalledVersion	FixedVersion
CRITICAL	CVE-2021-43527 (https://nvd.nist.gov/vuln/detail/CVE-2021-43527)	Memory corruption in decodeECorDsaSignature with DSA signatures (and RSA-PSS)	nss	3.67.0-6.el8_4	3.67.0-7.el8_5
CRITICAL	CVE-2021-43527 (https://nvd.nist.gov/vuln/detail/CVE-2021-43527)	Memory corruption in decodeECorDsaSignature with DSA signatures (and RSA-PSS)	nss-softokn	3.67.0-6.el8_4	3.67.0-7.el8_5
CRITICAL	CVE-2021-43527 (https://nvd.nist.gov/vuln/detail/CVE-2021-43527)	Memory corruption in decodeECorDsaSignature with DSA signatures (and RSA-PSS)	nss-softokn-freebl	3.67.0-6.el8_4	3.67.0-7.el8_5
CRITICAL	CVE-2021-43527 (https://nvd.nist.gov/vuln/detail/CVE-2021-43527)	Memory corruption in decodeECorDsaSignature with DSA signatures (and RSA-PSS)	nss-sysinit	3.67.0-6.el8_4	3.67.0-7.el8_5
CRITICAL	CVE-2021-43527 (https://nvd.nist.gov/vuln/detail/CVE-2021-43527)	Memory corruption in decodeECorDsaSignature with DSA signatures (and RSA-PSS)	nss-util	3.67.0-6.el8_4	3.67.0-7.el8_5
CRITICAL	CVE-2021-42575 (https://nvd.nist.gov/vuln/detail/CVE-2021-42575)	improper policies enforcement may lead to remote code execution	com.googlecode.owasp-java-html-sanitizer:owasp-java-html-sanitizer	20191001.1	20211018.2
CRITICAL	CVE-2021-23463 (https://nvd.nist.gov/vuln/detail/CVE-2021-23463)	XXE injection vulnerability	com.h2database:h2	1.4.197	2.0.202
CRITICAL	CVE-2021-42392 (https://nvd.nist.gov/vuln/detail/CVE-2021-42392)	h2: Remote Code Execution in Console	com.h2database:h2	1.4.197	2.0.206
CRITICAL	CVE-2022-23221 (https://nvd.nist.gov/vuln/detail/CVE-2022-23221)	Loading of custom classes from remote servers through JNDI	com.h2database:h2	1.4.197	2.1.210
CRITICAL	CVE-2022-46364 (https://nvd.nist.gov/vuln/detail/CVE-2022-46364)	SSRF Vulnerability	org.apache.cxf:cxf-core	3.3.10	3.4.10, 3.5.5
CRITICAL	CVE-2022-45047 (https://nvd.nist.gov/vuln/detail/CVE-2022-45047)	Java unsafe deserialization vulnerability	org.apache.sshd:sshd-common	2.3.0	2.9.2
CRITICAL	CVE-2022-45047 (https://nvd.nist.gov/vuln/detail/CVE-2022-45047)	Java unsafe deserialization vulnerability	org.apache.sshd:sshd-common	2.3.0	2.9.2
CRITICAL	CVE-2022-45047 (https://nvd.nist.gov/vuln/detail/CVE-2022-45047)	Java unsafe deserialization vulnerability	org.apache.sshd:sshd-common	2.3.0	2.9.2
CRITICAL	CVE-2022-45047 (https://nvd.nist.gov/vuln/detail/CVE-2022-45047)	Java unsafe deserialization vulnerability	org.apache.sshd:sshd-common	2.4.0	2.9.2
CRITICAL	CVE-2022-1245 (https://nvd.nist.gov/vuln/detail/CVE-2022-1245)	Privilege escalation vulnerability on Token Exchange	org.keycloak:keycloak-saml-core-public	15.0.2	18.0.0
CRITICAL	CVE-2022-0839 (https://nvd.nist.gov/vuln/detail/CVE-2022-0839)	Improper Restriction of XML External Entity	org.liquibase:liquibase-core	3.5.5	4.8.0
CRITICAL	CVE-2022-21724 (https://nvd.nist.gov/vuln/detail/CVE-2022-21724)	jdbc-postgresql: Unchecked Class Instantiation when providing Plugin Classes	org.postgresql:postgresql	42.2.5	42.2.25, 42.3.2
CRITICAL	CVE-2022-26520 (https://nvd.nist.gov/vuln/detail/CVE-2022-26520)	postgresql-jdbc: Arbitrary File Write Vulnerability	org.postgresql:postgresql	42.2.5	42.3.3
CRITICAL	CVE-2022-1471 (https://nvd.nist.gov/vuln/detail/CVE-2022-1471)	Constructor Deserialization Remote Code Execution	org.yaml:snakeyaml	1.26	2.0

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/IQB-NetApp/wiki/dockerhub.hi.inet-evolved-5g-validation-iqb-netapp-iqb-netapp-keycloak

USE OF 5G APIs

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

Repo used for Validation: **https://github.com/EVOLVED-5G/IQB-NetApp**
Branch used for Validation: evolved5g
Last commit ID: 9ede78aa0e55e85456146733b2b67e59abc5a161
Environment used: **kubernetes-uma**
Build number at Jenkins: 912

The individual result of the validations test is 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-monitoring-event/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

evolved 5G

Network App Validation Report: TeleopNetApp

Date: 29/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **TeleopNetApp** version **4.1**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/TeleopNetApp**
Branch used for Validation: evolved5g
Last commit ID: c88cc755362b0a5610f3005fccbde1e2489ecbd2
Environment used: **kubernetes-uma**
Build number at Jenkins: 945
Network App deploy time KPI: **22 seconds**
Total validation time: **31 Min**

The result of the Validation Process over the Network App **TeleopNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App TeleopNetApp has been validated

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

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/TeleopNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c88cc755362b0a5610f3005fccbde1e2489ecbd2

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

Scan of teleopnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	0
major	4
minor	1

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-teleopnetapp-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/TeleopNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c88cc755362b0a5610f3005fccbde1e2489ecbd2

The security scan has been performed using Trivy version 0.35.0

Scan of repo: TeleopNetApp

Summary

Severity	Number of vulnerabilities
HIGH	1
MEDIUM	1

Good work. Network App code does not have any security issue.

The Source Code Security Analysis has been completed successfully

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

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/TeleopNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c88cc755362b0a5610f3005fccbde1e2489ecbd2

Summary

Rule	Number of secrets leaked
Dominios expuestos	16

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	al-robotics-capif.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/environment.yaml#L8-L8)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	/pal-robotics-nef.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/environment.yaml#L9-L9)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	/pal-robotics-nef.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/environment.yaml#L10-L10)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	al-robotics-capif.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/environment.yaml#L13-L13)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	/pal-robotics-nef.apps.ocp-epg.hi.inet	K8s/environment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/environment.yaml#L16-L16)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	pal-robotics-nef.apps.ocp-epg.hi.inet	K8s/deployment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/deployment.yaml#L101-L101)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	al-robotics-capif.apps.ocp-epg.hi.inet	K8s/deployment.yaml (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/f4d621341f6b153f197782744c0d8b8ed0565dde/K8s/deployment.yaml#L102-L102)	Evolved5G	2023-07-19 09:31
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 09:54
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-TeleopNetApp/blob/3dc4c39863c271d5ea9867983a158794c66a7507/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-09-19 09:54

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/TeleopNetApp/wiki/secrets-Telefonica-Evolved5g-TeleopNetApp

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/TeleopNetApp Network apps are composed of the following services:

- teleopnetapp

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
teleopnetapp		

Publication of Network App docker images

Urls of Images published:

Image: **teleopnetapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/teleopnetapp:4.1
- dockerhub.hi.inet/evolved-5g/validation/teleopnetapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:teleopnetapp-4.1
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:teleopnetapp-latest

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **TeleopNetApp** version **4.1**

Repo used for Validation: **https://github.com/EVOLVED-5G/TeleopNetApp**
Branch used for Validation: evolved5g
Last commit ID: c88cc755362b0a5610f3005fccbde1e2489ecbd2
Environment used: **kubernetes-uma**
Build number at Jenkins: 945

The individual result of the validations test is 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-monitoring-event/***	SUCCESS
NEF SERVICES LOGGED AT CAPIF ***/nef/api/v1/3gpp-as-session-with-qos/***	SUCCESS
TSN SERVICES LOGGED AT CAPIF ***/tsn/api/***	SUCCESS

Congratulations usage of all 5G APIs has been successful

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/TeleopNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c88cc755362b0a5610f3005fccbde1e2489ecbd2

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
Apache Software License	3
MIT License	4
BSD License	1
Apache Software License;; MIT License	1

Dependencies Results

Compatible	Package	Version	License
✔	evolved5g	1.0.13	Apache Software License
✔	fastapi	0.103.2	MIT License
✔	fastapi_utils	0.2.1	MIT License
✔	flask	2.3.3	BSD License
✔	flask-cors	4.0.0	MIT License
✔	httptools	0.6.0	MIT License
✔	requests	2.31.0	Apache Software License
✔	uvloop	0.17.0	Apache Software License;; MIT License
✔	watchdog	3.0.0	Apache Software License

evolved
5G

Network App Validation Report: LocalizationNetApp

Date: 29/09/2023

VALIDATION REPORT EXECUTIVE SUMMARY

This Validation Report contains the results of the Validation process executed over the Network App **LocalizationNetApp** version **4.1**

Validation triggered by usuario_Evolved5G / usu_evolved5g
Repo used for Validation: **https://github.com/EVOLVED-5G/LocalizationNetApp**
Branch used for Validation: evolved5g
Last commit ID: c04adbec97c4085264dfc79aef76f61cac1b162e
Environment used: **kubernetes-uma**
Build number at Jenkins: 942
Network App deploy time KPI: **24 seconds**
Total validation time: **32 Min**

The result of the Validation Process over the Network App **LocalizationNetApp** has been: **SUCCESS**

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

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

Congratulations your Network App LocalizationNetApp has been validated

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

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/LocalizationNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c04adbec97c4085264dfc79aef76f61cac1b162e

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

Scan of localizationnetapp

Summary

Severity	Number of vulnerabilities
blocker	0
critical	1
major	2
minor	4

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-localizationnetapp-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/LocalizationNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c04adbec97c4085264dfc79aef76f61cac1b162e

The security scan has been performed using Trivy version 0.35.0

Scan of repo: LocalizationNetApp

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/LocalizationNetApp/wiki/Telefonica-Evolved5g-LocalizationNetApp

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/LocalizationNetApp
Branch used for the Analysis: evolved5g
Last Commit ID: c04adbec97c4085264dfc79aef76f61cac1b162e

Summary

Rule	Number of secrets leaked
Dominios expuestos	9

Passwords detected in commit history

Severity	Description	Match	File	Author	Date
low	Dominios expuestos	image = "dockerhub.hi.inet	iac/terraform/main.tf (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/iac/terraform/main.tf#L12-L12)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	ACTORY_CREDENTIALS}" dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/pac/Jenkins-build.groovy#L43-L43)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/pac/Jenkins-build.groovy#L44-L44)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	lved-5g/dummy-netapp dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/pac/Jenkins-build.groovy#L45-L45)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	mage push --all-tags dockerhub.hi.inet	pac/Jenkins-build.groovy (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/pac/Jenkins-build.groovy#L46-L46)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	FROM dockerhub.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/iac/slave/Dockerfile#L4-L4)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	te --quiet https://artifactory.hi.inet	iac/slave/Dockerfile (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/iac/slave/Dockerfile#L77-L77)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-deploy.groovy (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/pac/Jenkins-deploy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-12-22 10:04
low	Dominios expuestos	FT_URL= 'https://openshift-epg.hi.inet	pac/Jenkins-destroy.groovy (https://github.com/Telefonica/Evolved5g-LocalizationNetApp/blob/4e4135e527027d9c08b68c39e05229f9139553d2/pac/Jenkins-destroy.groovy#L13-L13)	Alejandro Molina Sanchez	2022-12-22 10:04

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/LocalizationNetApp/wiki/secrets-Telefonica-Evolved5g-LocalizationNetApp

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/LocalizationNetApp Network apps are composed of the following services:

- localizationnetapp

Check Ports Exposed Result

Each individual service that exposes a port are checked:

Service Name	Port	Status
localizationnetapp		

Publication of Network App docker images

Urls of Images published:

Image: **localizationnetapp**

Evolved-5G open repository:

- dockerhub.hi.inet/evolved-5g/validation/localizationnetapp:4.1
- dockerhub.hi.inet/evolved-5g/validation/localizationnetapp:latest

Evolved-5G AWS Docker Registry:

- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:localizationnetapp-4.1
- 709233559969.dkr.ecr.eu-central-1.amazonaws.com/evolved5gvalidation:localizationnetapp-latest

USE OF 5G APIs

This section will show all usage of 5G APIs of the Network App **LocalizationNetApp** version **4.1**

Repo used for Validation: **https://github.com/EVOLVED-5G/LocalizationNetApp**
Branch used for Validation: evolved5g
Last commit ID: c04adbec97c4085264dfc79aef76f61cac1b162e
Environment used: **kubernetes-uma**
Build number at Jenkins: 942

The individual result of the validations test is 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

evolved 5G