ETSI TS 133 527 V18.2.0 (2024-05)

5G;
Security Assurance Specification (SCAS)
for 3GPP virtualized network products
(3GPP TS 33.527 version 18.2.0 Release 18)

Reference
DTS/TSGS-0333527vi20

Keywords
5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document contains objectives, requirements and test cases to virtualized network product classes.

Several virtualized network product classes share very similar if not identical security requirements for some aspects. Therefore, these are collected in the present document applicable to many virtualized network product classes. In addition to this catalogue, requirements specific to different network product classes will be captured in separate documents.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[3] 3GPP TR 33.927: "Security Assurance Specification (SCAS); threats and critical assets in 3GPP virtualized network product classes".

[4] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[5] Void

[6] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[7] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

4 Catalogue of security requirements and related test cases for virtualized network product

4.1 Introduction

4.1.1 Pre-requisites for testing

The SCAS tests, as described in the present specification, are to be applied to a virtualized network product whose software and/or hardware has been brought into use so that the network product can provide the intended functionality, either in a real network environment or in a simulated environment. This implies that, before any testing is performed, the software and/or hardware has been installed correctly, the virtualized network product is instantiated, and communication has been established over all standardized interfaces and OAM interfaces related with the network product's functionality, as described in the vendor's documentation. In addition, supporting environment for GVNP has also been provided before the testing is performed. The assumption of requirement for the NFVI supporting environment have been included in the vendor's documentation.

Communication over external non standardized interfaces that may exist and are marked as optional, according to the vendor's documentation, shall also be established during testing unless they are explicitly marked as "not recommended" in the vendor's documentation.

For each of the enabled external communication interfaces there may be various optional capabilities. During testing, all such capabilities shall be enabled unless they are explicitly marked as "not recommended" in the vendor's documentation.

In some cases a test case might require configuration changes as part of the execution steps or pre-conditions. After such test is executed and prior to any further test execution it needs to be ensured that the state of the ToE is restored back in the original state.

SCAS testing is not about security in operations and deployments. So, in particular, SCAS testing is independent of any operator guidelines or considerations on specific deployment scenarios.

4.1.2 Use of tools in testing

The following text shall apply to all test cases described in the present document:

The present document takes into account that the landscape of testing tools evolves more rapidly than SCAS specifications. It is therefore allowed that, for each requirement, the actual test carried out may deviate from the stepwise description of the test case in the present document if the following conditions are fulfilled:

(1) The test is carried out by preferably using Commercial-of-the-Shelf (COTS) and Free-Open-Source-Software (FOSS) tools that are available for other testers that may want to repeat the test. In case a tool not in any of these two categories is used then evidence of the quality assurance of the tool needs to be provided. This applies only to tools used to perform the actual test and not supportive tools needed for setting up the testing environment like for example traffic generators/ simulators.

In cases where a test lab is not able to obtain the necessary tools to perform the test, vendor proprietary test tools may be used by the test lab as long the test tool is controlled under a suitable quality management system (QMS). The test lab ensures that this QMS is in place in order to avail of a vendor’s test tool.

Additionally in cases where the accredited test lab does not have the necessary test environment to perform a test, it shall be possible for the accredited test lab personnel to perform the test in a vendor's test lab. In such cases the accredited lab should record details of test environment, test set-up used and how the test was performed.

(2) The tester provides evidence, e.g. by referring to the documentation of the tool, that the tool is suitable to verify the requirement, and the scope of testing is equal or larger to the one of the test case described in the present document. The evidence needs to be sufficiently detailed for experts in the field of testing, not for the general public.

(3) The tester provides evidence that the tool has been actually used for testing the network product (e.g. by providing a trace).

4.1.3 Documentation Requirements

When a test case makes an assumption on the availability of certain items in the product documentation then this assumption is to be considered part of the requirement even if the requirements text does not mention the documentation.

4.2 Security functional requirements and related test cases

4.2.1 Introduction

The present clause describes security functional requirements and the corresponding test cases, independent of a specific virtualized network product class of type 1. According to security threat analysis in TR 33.927 [2], the proposed security requirements for GVNP of type 1 are classified in three groups:

- Security functional requirements deriving from 3GPP specifications in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in the 3GPP specifications but whose support is also important to ensure a network product conforms to a common security baseline detailed in clause 4.2.3.3.5.
- Security functional requirements related to Virtualization layer, hardware and resource isolation, among others. These requirements can be called security functional requirements deriving virtualization for simplify and detailed in clause 4.2.7.

Compared to physical network products, GVNP of type 1 faces the threats relating to ETSI-definer interfaces defined in [3] and [4]. So, the security requirements of the above first and second group shall base on the security requirements in clause 4.2 of TS 33.117 [1] to identify the different security requirements for GVNP of type 1.

4.2.2 Security functional requirements deriving from 3GPP specifications and related test cases

Clause 4.2.2 in TS33.117[1] can be reused. There are no VNF-specific additions to clause 4.2.2 of TS 33.117 [1].

4.2.3 technical baseline

4.2.3.1 Introduction

The technical baseline in clause 4.2.3 of TS33.117[1] is a generic set of security requirements to be fulfilled by all virtualized network products.

In particular these requirements counter the security threats identified in the TR 33.927 [2] and they basically aim to guarantee the network product confidentiality, integrity and availability.

4.2.3.2 Protecting data and information

All text from TS 33.117 [1], clause 4.2.3.2 applies to GVNP of type 1.

4.2.3.3 Protecting availability and integrity

4.2.3.3.1 System handling during overload situations

All text from TS 33.117 [1], clause 4.2.3.3.1 applies to GVNP of type 1.

4.2.3.3.2 Boot from intended memory devices only

All text from TS 33.117[1], clause 4.2.3.3.2 applies to GVNP of type 1.

4.2.3.3.3 System handling during excessive overload situations

All text from TS 33.117 [1], clause 4.2.3.3.3 applies to GVNP of type 1.

4.2.3.3.4 System robustness against unexpected input

All text from TS 33.117 [1], clause 4.2.3.3.4 applies to GVNP of type 1.

4.2.3.3.5 Virtualized Network product software package integrity

4.2.3.3.5.1 Overview

All text from TS 33.117 [1], clause 4.2.3.3.5 applies to GVNP of type 1.

In addition, VNF package and VNF image integrity shall be validated when on board, and VNF image integrity shall be validated when in instantiated. The detailed potential security requirements and related test cases are as following.

4.2.3.3.5.2 VNF package and VNF image integrity

Requirement Name: VNF package and VNF image integrity

Requirement Description:

1) VNF package and image shall contain integrity validation value (e.g. MAC).

2) VNF package shall be integrity protected during on boarding.

Threat Reference: Clause 5.3.2.5.1 of the TR 33.927[2], "Software Tampering ";

Test case:

Test Name: TC_VNF PACKAGE AND IMAGE_ INTEGRITY

Purpose:

1. To test whether the VNF package has been integrity protected or not.

2. To test whether the VNF image has been integrity protected or not.

Procedure and execution steps:

Pre-Condition:

- The virtualized network product document describes information regarding integrity protection of VNF package and VNF images, including details of how the integrity check is carried out, who makes the digital signatures of VNF package, what evidence is created to prove that the integrity check has been executed and what the result of the check is, etc.

- A valid VNF package and a not-valid VNF package (i.e. a tampered image in VNF package) are available.

- A valid VNF image (i.e. a correct HASH value is attached) and a not-valid VNF image (i.e. an incorrect HASH value is attached, e.g. the VNF image can be tampered when the VNF image is sent from the NFVO to the VIM or when the VNF image is stored in the image repository) are available in the image repository of VIM.

- There are NFVO and VIM, or simulated NFVO and VIM. The certificate or the public key which is used to verify the digital signature of VNF package and image has been pre-configured in the NFVO and VIM respectively.

Execution Steps

Execute the following steps:

1. Review the documentation provided by the vendor describing how VNF package integrity is verified;
2. During VNF package on boarding, the tester uploads a valid VNF package into a NFVO. The NFVO verifies the integrity of the VNF package by validating the digital signature of the VNF package using the pre-configured certificate or public key according to the documentation;
3. During VNF package on boarding, the tester uploads a not-valid VNF package into a NFVO. The NFVO validates the digital signature of the VNF package using the pre-configured certificate or public key;
4. During VNF instantiation, the VIM selects a VNF image with a correct integrity protection value from the image repository to instantiate the VNF image. The VIM validates the correctness of the integrity protection value using the pre-configured certificate or public key according to the documentation;
5. During VNF instantiation, the VIM selects a VNF image with an incorrect integrity protection value from the image repository to instantiate the VNF image. The VIM validates the correctness of the integrity protection value using the pre-configured certificate or public key according to the documentation.

Expected Results:

1. The VNF package is successfully on boarded into the NFVO;
2. The not-valid VNF package is not on boarded;
3. The VNF image with a correct integrity protection value is instantiated by the VIM;
4. The VNF image with an incorrect integrity protection value is not instantiated by the VIM.

Expected format of evidence:

Snapshots containing the result of the VNF package on boarding and the VNF image instantiation.

4.2.3.4 Authentication and authorization

All text from TS 33.117 [1], clause 4.2.3.4 applies to virtualized network products.

4.2.3.5 Protecting sessions

All text from TS 33.117 [1], clause 4.2.3.5 applies to virtualized network products.

4.2.3.6 Logging

All text from TS 33.117 [1], clause 4.2.3.6 applies to virtualized network products.

4.2.4 Operating systems

All text from TS 33.117 [1], clause 4.2.4 applies to guest operating systems for GVNP of type 1.

4.2.5 Web servers

All text from TS 33.117 [1], clause 4.2.5 applies to GVNP of type 1.

4.2.6 Network devices

All text from TS 33.117 [1], clause 4.2.6 applies to GVNP of type 1.

4.2.7 Security functional requirements deriving from virtualisation and related test cases

4.2.7.1 Security functional requirements on GVNP lifecycle management

Requirement Name: GVNP lifecycle management security

Requirement Description:

1) VNF shall authenticate VNFM when VNFM initiates a communication to VNF.

2) VNF shall be able to establish securely protected connection with the VNFM.

3) VNF shall check whether VNFM has been authorized when VNFM access VNF's API.

4) VNF shall log VNFM's management operations for auditing.

NOTE: According to the definition in ETSI GS NFV 003 [6], VNFM is responsible for the lifecycle management of VNF. The lifecycle management of VNF is set of functions required to manage the instantiation, maintenance and termination of VNF. The GVNP of type 1 is 3GPP VNF. A 3GPP VNF lifecycle management begins when the 3GPP VNF is instantiated by a VNFM after the 3GPP VNF package is delivered to the operator and uploaded to NFVO. It is different terminology with the product lifecycle management process in clause 6 that includes set of functions required to manage first commercial introduction, update, minor release, major release, end of life.

Threat Reference: Threats on interface between 3GPP VNF and VNFM, in clause 5.3.2.3 of TR 33.927 [3].

Test case:

Test Name: TC_LIFECYCLE MANAGEMENT SECURITY

Purpose:

1. To test the VNF authenticates VNFM when VNFM initiates a communication to VNF.

2. To test the VNF establishes secure connection with the VNFM after successful authentication.

3. To test the VNF check whether VNFM has been authorized when VNFM access to VNF's API.

4. To check whether VNF logs the lifecycle management operations from VNFM.

NOTE: Void

Procedure and execution steps:

Pre-Condition:

NOTE: If the interface between VNF and VNFM is not exposed and not accessible, execution steps 1-5 are not applicable. If the interface between VNF and VNFM is proprietary, the vendor provides as much and as detailed information on the interface implementation so that the tester is able to verify the interfaces security requirements.

1. There is a VNFM (or simulated VNFM) in the test environment.

2. The VNF vendor's document describes how VNF authenticates/authorizes VNFM. Execution Steps

Execute the following steps:

1. The tester triggers the establishment of communication between the VNF and the VNFM.

2. The tester captures the communication between the VNF and the VNFM using a tool (e.g. wireshark).

3. The tester checks whether the VNF authenticates the VNFM or not according to the mechanism described in the vendor's document. For example, the VNF can use HTTPS to communicate with the VNFM, the VNF uses VNFM's certificate for authentication.

4. The tester checks whether the VNF establishes secure connection with the VNFM after successful authentication. For example, a TLS connection is established after the VNF successfully authenticates the VNFM.

5. The tester using the VNFM to access the VNF's API and checks whether the VNF authorizes the VNFM or not according to the mechanism described in the vendor's document. For example, VNF can use OAuth2.0 to authorize the VNFM. The VNF uses VNFM's token for authorization.

6. The tester checks whether the VNF logs the operations from VNFM or not.

Expected Results:

1. Secure communication is established between VNF and VNFM with integrity and confidentiality protection.

2. The VNFM successfully accesses the VNF's API.

3. The VNF logs the operations from VNFM.

Expected format of evidence:

1. Pcap traces contain the authentication and authorization processes.

2. Screenshot contains the logs.

4.2.7.2 Security functional requirements on executive environment provision

Requirement Name: secure executive environment provision

Requirement Description:

The VNF shall support to compare the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.

Threat Reference: Threats on interface between 3GPP VNF and virtualisation layer, in clause 5.3.2.3 of TR 33.927 [3].

Test case:

Test Name: TC_SECURE EXECUTIVE ENVIRONMENT PROVISION

Purpose:

1. To test whether the VNF compares the owned resource state with the parsed resource state.

2. To test whether the VNF send an alarm to the OAM if the two resource states are inconsistent.

Procedure and execution steps:

Pre-Condition:

There are a VNF, a virtualization layer (or simulated virtualization layer), an OAM, a VNFM, a VIM (or simulated OAM, VNFM, VIM) on the test environment.

Execution Steps

Execute the following steps:

1. The tester utilizes the virtualization layer to change the resource state of VNF (e.g. change vCPU size of the VNF).

2. The tester uses the VNF to query the parsed resource state from the OAM.

3. The tester uses the OAM to query the parsed resource state of the VNF from the VNFM and send the received resource state to the VNF.

4. The tester checks whether the VNF sends an alarm to the OAM when the VNF receives the parsed resource state from the OAM and finds that the owned resource state and the parsed resource state are inconsistent.

Expected Results:

1. The VNF send an alarm to the OAM when the VNF receives the parsed resource state from the OAM and find that the owned resource state and the parsed resource state are inconsistent.

Expected format of evidence:

1. Screenshot contains the alarm on the OAM.

4.2.7.3 Instantiating VNF from trusted VNF image

Requirement Name: Instantiating VNF from trusted VNF image

Requirement Description:

A VNF shall be initiated from trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the operators.

Threat Reference: TR 33.926 [7], Clause5.3.4.1, "Software Tampering ";

Test case:

Test Name: TC_INSTANTIATING VNF _ TRUSTED IMAGE

Purpose:

To test whether the instantiating VNF from trusted VNF image.

Procedure and execution steps:

Pre-Condition:

- The virtualized network product document describes information regarding digital signature protection of VNF images, including details of how the signature check is carried out, who makes the digital signature of VNF image etc.
- One VNF package included two trusted VNF images and the VNF package carries a correct digital signature of the VNF package.
- Another VNF package included untrusted VNF image which carry wrong digital signature of VNF image and the VNF package carries a correct digital signature of the VNF package.
- There are a NFVO, or a simulated NFVO. A certificate or public key which is used to verify the digital signature of VNF image has been pre-configured in the NFVO. This certificate is trusted by the operator. It means the digital signature of the VNF image is successfully verified by using the public key in the certificate trusted by the operator

Execution Steps:

Execute the following steps:

1. Review the documentation provided by the vendor describing how digital signature of the VNF image is verified;
2. The tester uploads a VNF package included two trusted VNF images into a NFVO. The NFVO verifies the VNF images by validating each digital signature of the VNF image using the pre-configured certificate or the public key according to the documentation;
3. The tester uploads another VNF package included un-trusted VNF image into NFVO. The NFVO verifies the VNF image(s) by validating each digital signature of the VNF image using the pre-configured certificate or the public key according to the documentation.

NOTE: The digital signature validation of the image is also described in clause 4.2.3.3.5.2 VNF package and VNF image integrity, but the two test cases have the different test purposes. This test case focuses on VNF image credibility, while clause 4.2.3.3.5.2 is concerned with VNF image integrity.

Expected Results:

1. In the step 2, the signatures of the VNF images are successfully validated and the VNF package is successfully on boarded into the NFVO;
2. In the step 3, the signature of the un-trusted VNF image is failed to be validated and the VNF package is not on boarded into the NFVO;

Expected format of evidence:

Snapshots containing the result of the VNF package on boarding.

4.3 Security requirements and related test cases related to hardening

4.3.1 Introduction

The requirements proposed in the present clause aim to securing virtualised network products (including the network functions in service-based architecture) by reducing its surface of vulnerability. In particular the identified requirements aim to ensure that all the default virtualised network product configurations (including operating system software, firmware and applications) are appropriately set. The hardening requirements were proposed in TS 33.117 [2] are general and generally apply to GVNP of type 1. So, the potential hardening requirements for GVNP of type 1 also include four aspects, i.e. general hardening requirements (i.e. technical baseline), operating system, web server, network devices.

Compared to the physical network products, GVNP of type 1 has not hardware, but contains 3GPP functions, other functions and guest OS, it also has inter-VNF traffic and intra-VNF traffic in addition to than O&M traffic, control plane traffic and data plane traffic etc. The following clauses describe how to reduce the exposure from these new features.

4.3.2 Technical baseline

4.3.2.1 No unnecessary or insecure services / protocols

All text from TS 33.117 [2], clause 4.3.2.1 applies to GVNP of type 1.

4.3.2.2 Restricted reachability of services

All text from TS 33.117 [2], clause 4.3.2.2 applies to GVNP of type 1.

4.3.2.3 No unused software

All text from TS 33.117 [2], clause 4.3.2.3 applies to GVNP of type 1.

4.3.2.4 No unused functions

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [2] clause 4.3.2.4 applies to GVNP of type 1, except the requirements and testing on hardware functions.

4.3.2.5 No unsupported components

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [2] clause 4.3.2.5 applies to GVNP of type 1, except the requirements and testing on hardware components.

4.3.2.6 Remote login restrictions for privileged users

All text from TS 33.117 [2], clause 4.3.2.6 applies to GVNP of type 1.

4.3.2.7 File system Authorization privileges

All text from TS 33.117 [2], clause 4.3.2.7 applies to GVNP of type 1.

4.3.3 Operating systems

All text from TS 33.117 [2], clause 4.2.4 applies to guest operating systems for GVNP of type 1.

4.3.4 Web servers

All text from TS 33.117 [2], clause 4.2.5 applies to GVNP of type 1.

4.3.5 Network devices

All text from TS 33.117 [2], clause 4.2.6 applies to GVNP of type 1.

4.3.6 Virtualized Network Products

4.3.6.1 Traffic separation

All text from TS 33.117 [2], clause 4.3.5.1 applies to GVNP of type 1, except for the supporting physical separation of traffic belonging to different network domains. However, the supporting separation of traffic belonging to different network domain shall be supported for virtualized network products. It needs to have same testing step but to set Pre-condition from two separate interface to two separate logical interface from TS 33.117 [2].

4.3.6.2 Separation of inter-VNF and intra-VNF traffic

Requirement Name: inter-VNF and intra-VNF Traffic Separation

Requirement Description:

The network used for the communication between the VNFCIs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affect each other.

Threat Reference: Security threat caused by lack of GVNP traffic isolation in clause 5.3.2.7.15 of TR 33.927 [3]

Test case:

Test Name: TC_TRAFFIC_SEPARATION_INTER-VNF_INTRA-VNF

Purpose:

To test whether the traffics between inter-VNF traffic and intra-VNF traffic are separated.

Procedure and execution steps:

Pre-Condition:

1. There has a VNF instance on the test environment. This VNF instance has more than one VNFCI (VNF component Instance). The network between VNFCIs means intra-VNF network which is private network provided by vendor.
2. The document which describes how to separate the inter-VNF traffic with the intra-VNF traffic has been provided by the vendor. For example, the different network segments are described in the document.
3. Another VNF instance (or a simulated VNF instance) is on the test environment and can communicate with the tested VNF instance.

Execution Steps

Execute the following steps:

1. The tester checks whether the inter-VNF traffic and intra-VNF traffic are separated according the document by the vendor. For example, the tester checks whether the different network segments used by inter-VNF traffic and intra-VNF traffic respectively.
2. The tester checks whether a VNFCI refuses inter-VNF traffic on all intra-VNF interfaces. For example, the tester can send ping to all intra-VNF interfaces through an inter-VNF interface.
3. The tester checks whether a VNFCI refuses intra-VNF traffic on all inter-VNF interfaces. For example, the tester can send ping to all inter-VNF interfaces through an intra-VNF interface.

Expected Results:

In the step 1, the inter-VNF traffic and intra-VNF traffic are separated according the document by the vendor. In the step 2 and step 3, the VNFCI refuses traffic.

Expected format of evidence:

A PASS or FAIL.

4.4 Basic vulnerability testing requirements

4.4.1 Introduction

All text from TS 33.117 [2], clause 4.4 applied to all types of GVNPs.

4.4.2 Port Scanning

All text from TS 33.117 [2], clause 4.4.2 applied to all types of GVNPs.

4.4.3 Vulnerability Scanning

All text from TS 33.117 [2], clause 4.4.3 applied to all types of GVNPs.

4.4.4 Robustness and Fuzz testing

All text from TS 33.117 [2], clause 4.4.4 applied to all types of GVNPs.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-06	SA#100					Upgrade to change control version	18.0.0
2023-06	SA#100					EditHelp review	18.0.1
2023-12	SA#102	SP-231346	0001		F	Correction for VNF package and VNF image integrity of clause 4.2.3.3.5.2	18.1.0
2024-03	SA#103	SP-240364	0003	1	D	Fixed typo in VNF traffic separation test case	18.2.0
2024-03	SA#103	SP-240364	0004	-	F	Removal of note in GVNP lifecyle management	18.2.0

History

Document history		
V18.2.0	May 2024	Publication