ETSI GS NFV-SEC 028 V5.1.1 (2024-05)

Network Functions Virtualisation (NFV) Release 5; Security; Security Assurance Specification (SCAS) for Generic NFV-MANO

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGS/NFV-SEC028ed511

Keywords
MANO, NFV, SCAS, security, test

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

Contents

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.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

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.

1 Scope

The present document defines the security assurance of generic NFV-MANO products. The outcome of the present document expects the security assets, security threats, security requirements and test cases for evaluating the generic security of NFV-MANO products. In the present document, the security assurance methodology introduced in 3GPP specifications will be leveraged. Security test cases including testing goals, testing steps, and evidence of testing results will be produced for evaluating whether the security requirements are implemented by NFV-MANO products.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 133 117: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Catalogue of general security assurance requirements (3GPP TS 33.117)".

[2] ETSI GS NFV-SOL 013: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs".

[3] ETSI GS NFV-SEC 022: "Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access".

[4] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[5] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[6] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[7] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 133 926: "LTE; 5G; Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (3GPP TR 33.926)".

[i.2] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.3] ETSI TR 133 916: "LTE; 5G; Security Assurance Methodology (SCAM) for 3GPP network products (3GPP TR 33.916)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.2] and the following apply:

Basic Vulnerability Testing (BVT): process of running security tools against a network product

NOTE: BVT is defined by the use of Free and Open Source Software (FOSS) and Commercial Off-The-Shelf (COTS) security testing tools on the external interfaces of the network product.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.2] and the following apply:

CVE Common Vulnerabilities and Exposures

4 Catalogue of security requirements and related test cases for generic part of NFV-MANO products

4.1 Introduction

The present clause describes security functional requirements and the corresponding test cases for generic part of NFV-MANO products.

4.2 Security functional requirements and related test cases

4.2.1 Introduction

The present clause describes the security functional requirements and the corresponding test cases, independent of a specific NFV-MANO product class. In particular the proposed security requirements are classified in two groups:

- Security functional requirements deriving from ETSI specifications and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in the ETSI specifications but whose support is also important to ensure a NFV-MANO product conforms to a common security baseline detailed in clause 4.2.3.

By default all test cases in clause 4.2 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products. Any additions, deletions or modification are listed separately from clause 4.2.2 to clause 4.2.6.

4.2.2 Security functional requirements on the NFV-MANO deriving from ETSI specifications and related test cases

4.2.2.1 Security functional requirements deriving from ETSI NFV specifications - general approach

The present clause describes the general approach taken towards security functional requirements deriving from ETSI specifications and the corresponding test cases, independent of a specific network product class.

It is assumed for the purpose of the present SCAS that a network product conforms to all mandatory security-related provisions in ETSI specifications pertaining to it, in particular:

- all ETSI NFV SEC specifications (security specifications) that are pertinent to the network product class;
- other ETSI specifications that make reference to security specifications or are referred to from one of them.

Security procedures pertaining to a network product are typically embedded in non-security procedures and are hence assumed to be tested together with them.

It is the purpose of the present SCAS to identify security requirements from the NFV security architecture that require special attention in testing as they may:

a) lead to vulnerabilities when not satisfied;

b) not be captured through ordinary testing activity for non-security procedures;

c) address security-relevant failure cases and exceptions or 'negative' requirements of the kind: "The network product shall not…".

It is not an intention of the present document to provide an exhaustive set of test cases that would be sufficient to demonstrate conformance of all security procedures with the above-mentioned specifications.

4.2.2.2 Security functional requirements deriving from ETSI specifications - general Interface aspects

4.2.2.2.1 Introduction

The purpose of clauses 4.2.2.2.1 and 4.2.2.2.2 is to identify and describe the general baseline requirements from NFV security architecture and the corresponding test cases. The general baseline requirements are applicable to all NFV Management and Orchestration (MANO) functions.

4.2.2.2.2 Protection at the transport layer

Requirement Name: Protection at the transport layer

Requirement Reference: ETSI GS NFV-SOL 013 [2], clause 4.1, clause 8.1, clause 8.2.2, clause 8.2.5, clause 8.3.2, ETSI GS NFV-SEC 022 [3], clause 5.3.

Requirement Description:

"*APIs shall use TLS version 1.2 as defined by IETF RFC 5246 [4] or later. Versions of TLS earlier than 1.2 shall neither be supported nor used*". As specified in ETSI GS NFV-SOL 013 [2], clause 4.1.

"*As part of setting up the TLS tunnel for the access token request, the client and authorization server perform mutual authentication based on X.509 certificates. As part of the access token request, the client presents its client identifier*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.1.

"*In order to ensure that no third party can eavesdrop on sensitive information such as client credentials or access tokens, TLS is used to protect the transport of HTTP messages. If mutual authentication using TLS protocol is used, then the producer/server is authenticated to the consumer/client, but also the consumer/client is authenticated by the producer/server at the same time. To facilitate this mutual authentication, the server shall request a client certificate*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.1.

"*As a precondition for step 1 to succeed, a TLS channel has been set up between API consumer and authorization server. Unless the API consumer is allowed to use client password, the API consumer and the authorization server have mutually authenticated based on TLS certificates during TLS tunnel set-up*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.2.2.

"*Unless the API consumer is allowed to use client password, the API producer and the notification authorization server have mutually authenticated based on TLS certificates during TLS tunnel set-up*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.2.5.

"*As a precondition for the access token request to succeed, client and authorization server shall have mutually authenticated based on TLS certificates during TLS tunnel set-up, unless the use of client password is allowed for the client*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.3.2.

"*The TLS connection between the client and the authorization server token endpoint shall be established with mutual TLS X.509 certificate authentication, i.e. using certificate and certificate verify messages sent during the TLS Handshake*". As specified in ETSI GS NFV-SEC 022 [3], clause 5.3.

Threat References: ETSI GS NFV-SEC 012 [7], clause 6.5, weak cryptographic algorithms.

Test case:

Test Name: TC_PROTECT_TRANSPORT_LAYER

Purpose:

Verify that TLS protocol for NFV-MANO API mutual authentication and NFV-MANO API transport layer protection is implemented in the network products based on the profile required.

Procedure and execution steps:

Pre-Conditions:

Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

A peer implementing the TLS protocol configured by the vendor shall be available.

The tester shall base the tests on the requirements specified in clause 6.2.3 (if TLS version 1.2 as defined by IETF RFC 5246 [4] is used) or clause 6.2.2 (if TLS version 1.3 as defined by IETF RFC 8446 [5] is used) of ETSI TS 133 210 [6] (3GPP Release 16 or later).

Execution Steps

1) The tester shall check that compliance with the TLS profile can be inferred from detailed provisions in the network product documentation.

2) The tester shall establish a secure connection between the network product under test and the peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test. Additionally, verify that the certificate used by the product under test is signed by a trusted certificate authority.

3) The tester shall try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile or the certificate presented is not signed by a trusted certificate authority.

Expected Results:

- The network product under test and the peer establish TLS if the TLS profiles used by the peer are compliant with the requirements in clause 6.2.3 (if TLS version 1.2 as defined by IETF RFC 5246 [4] is used) or clause 6.2.2 (if TLS version 1.3 as defined by IETF RFC 8446 [5] is used) of ETSI TS 133 210 [6] and the server certificate is signed by a trusted certificate authority.

- The network product under test and the peer fail to establish TLS if the TLS profiles used by the peer are forbidden in clause 6.2.3 (if TLS version 1.2 as defined by IETF RFC 5246 [4] is used) or clause 6.2.2 (if TLS version 1.3 as defined by IETF RFC 8446 [5] is used) of ETSI TS 133 210 [6] or the certificate is not signed by a trusted certificate authority.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.3 Technical Baseline

4.2.3.1 Introduction

The present clause provides baseline technical requirements. All test cases in clause 4.2.3 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.2.4 Operating systems

4.2.4.1 General operating system requirements and related test cases

The present clause provides operating system requirements.

4.2.5 Web servers

4.2.5.1 General web servers' requirements and related test cases

The present clause provides web server requirements. All test cases in clause 4.2.5 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.2.6 Network devices

4.2.6.1 General network devices requirements and related test cases

The present clause provides network devices requirements. All test cases in clause 4.2.6 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products with the exceptions listed in clause 4.2.6.2.

4.2.6.2 GTP-C and GTP-U Filtering

4.2.6.2.1 GTP-C Filtering

The requirement and test case in clause 4.2.6.2.3 of ETSI TS 133 117 [1] is not applicable to generic NFV-MANO products.

4.2.6.2.2 GTP-U Filtering

The requirement and test case in clause 4.2.6.2.4 of ETSI TS 133 117 [1] is not applicable to generic NFV-MANO products.

4.3 Security requirements and related test cases related to hardening

4.3.1 Introduction

The present clause contains NFV-MANO adaptations of hardening requirements and related test cases.

4.3.2 Technical Baseline

4.3.2.1 Introduction

All test cases in clause 4.3.2 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products with the exceptions listed in clause 4.3.5 and clause 4.3.6.

4.3.3 Operating Systems

4.3.3.1 Introduction

All test cases in clause 4.3.3 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.3.4 Web Servers

4.3.4.1 Introduction

All test cases in clause 4.3.4 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.3.5 Network Devices

4.3.5.0 Introduction

All test cases in clause 4.3.5 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products with the exceptions listed in clause 4.3.5.1.

4.3.5.1 Traffic Separation

The requirement and test case in clause 4.3.5.1 of ETSI TS 133 117 [1] is not applicable to generic NFV-MANO products.

4.3.6 Network Functions in service-based architecture

4.3.6.0 Introduction

All test cases in clause 4.3.6 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products with the exceptions listed from clause 4.3.6.1 to clause 4.3.6.3.

4.3.6.1 No code execution or inclusion of external resources by JSON parsers

The requirement and test case in clause 4.3.6.2 of ETSI TS 133 117 [1] is not applicable to generic NFV-MANO products.

4.3.6.2 Unique key values in IEs

The requirement and test case in clause 4.3.6.3 of ETSI TS 133 117 [1] is not applicable to generic NFV-MANO products.

4.3.6.3 The valid format and range of values for IEs

The requirement and test case in clause 4.3.6.4 of ETSI TS 133 117 [1] is not applicable to generic NFV-MANO products.

4.4 Baseline vulnerability testing requirements

4.4.1 Introduction

All test cases in clause 4.4 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products with the exceptions listed in clause 4.4.5 and clause 4.4.6.

4.4.2 Port Scanning

All test cases in clause 4.4.2 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.4.3 Vulnerability Scanning

All test cases in clause 4.4.3 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.4.4 Robustness and fuzz testing

All test cases in clause 4.4.4 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products.

4.4.5 White/Grey Box Vulnerability Scanning

Requirement Name: White/Grey Box Vulnerability scanning

Requirement Description:

Where required in order to demonstrate compliance for requirements on cryptography, key storage, secure deletion, or implementation of protocols, etc. or where the expected attacker is considered having a higher potential white/grey box vulnerability scanning should be conducted (see clause 4.8 of ETSI TR 133 916 [i.3]).

The purpose of white/grey box vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans are in place to mitigate them) within the Network Product, both in the OS and in the applications installed, that can be detected by means of automatic testing tools. White/grey box vulnerability scanning can be conducted by tools with the ability to log into the Network Product and execute commands, commonly with elevated privileges.

Vulnerability scanning tools may also report false positives and they shall be investigated and documented in the test report.

The test for this requirement can be carried out using a suitable tool or manually performed as described below. If a tool is used then the tester needs to provide evidence, e.g. by referring to the documentation of the tool, that the tool actually provides functionality equivalent to the steps described below.

Test case:

Test Name: TC_BVT_WHITE-GREY_VULNERABILITY_SCANNING

Purpose:

The purpose of white/grey box vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans are in place to mitigate them) within the Network Product that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces or command line interface.

Procedure and execution steps:

Pre-Conditions:

A list of all available services containing at least the following information shall be included in the documentation accompanying the Network Product:

- all services providing IP-based protocols;

- the available transport layer protocols on these interfaces;
- their open ports and associated services;
- and a free-form description of their purposes.

NOTE 1: This list is to be validated as part of the BVT port scanning activity.

The used vulnerability scanning tool shall be capable to detect known vulnerabilities on common services. The used vulnerability information shall be reasonably recent at the time of testing.

Execution Steps

The accredited evaluator's test lab is required to execute the following steps:

1) Execution of the suitable vulnerability scanning tool against all interfaces providing IP-based protocols of the Network Product.
2) Where possible execution of the suitable vulnerability scanning tool against the command line with administrative/root privileges of the Network Product.
3) Evaluation of the results based on their severity.

Expected Results:

The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation.

The discovered vulnerabilities (including source, example CVE ID), together with a rating of their severity, shall be highlighted in the testing documentation.

COTS Vulnerability scanners, by their nature (e.g. depending on how they are configured) may result in false findings/positives. The tool's documentation may even mention that the failing test shall be repeated to check whether it is really a recurring problem or not. The tester shall make best effort to determine if there is an issue with NP or the test tool and if necessary, work with the vendor of the network product to come to a consensus on the test result outcome.

NOTE 2: This testing documentation is input to the vulnerability mitigation process (that may include patching). This is part of the product lifecycle management process.

Expected format of evidence:

Output of BVT tool.

4.4.6 Container Image Vulnerability Scanning

Requirement Name: Container Image Vulnerability scanning

Requirement Description:

The purpose of container image vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans are in place to mitigate them) within the Network Product, both in the container base/parent image and in the application layers, that can be detected by means of automatic testing tools. Container image vulnerability scanning can be conducted by tools with the ability to examine each layer of the image.

Vulnerability scanning tools may also report false positives and they shall be investigated and documented in the test report.

The test for this requirement can be carried out using a suitable tool or manually performed as described below. If a tool is used then the tester needs to provide evidence, e.g. by referring to the documentation of the tool, that the tool actually provides functionality equivalent to the steps described below.

Test case:

Test Name: TC_BVT_CONTAINER_IMAGE_VULNERABILITY_SCANNING

Purpose:

The purpose of container image vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans are in place to mitigate them) within the Network Product that can be detected by means of automatic testing tools via the container image contents.

Procedure and execution steps:

Pre-Conditions:

The used vulnerability scanning tool shall be capable to detect known vulnerabilities on detected software packages. The used vulnerability information shall be reasonably recent at the time of testing.

The image in this case shall be used to deploy containerized environment.

Execution Steps

The accredited evaluator's test lab is required to execute the following steps:

1) Execution of the suitable vulnerability scanning tool against all container images of the Network Product.

2) Evaluation of the results based on their severity.

Expected Results:

The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation.

The discovered vulnerabilities (including source, example CVE ID), together with a rating of their severity, shall be highlighted in the testing documentation.

COTS Vulnerability scanners, by their nature (e.g. depending on how they are configured) may result in false findings/positives. The tool's documentation may even mention that the failing test shall be repeated to check whether it is really a recurring problem or not. The tester shall make best effort to determine if there is an issue with NP or the test tool and if necessary, work with the vendor of the network product to come to a consensus on the test result outcome.

NOTE: This testing documentation is input to the vulnerability mitigation process (that may include patching). This is part of the product lifecycle management process.

Expected format of evidence:

Output of BVT tool.

Annex A (informative): Generic NFV-MANO class description

A.1 Overview

The present clause captures the generic NFV-MANO network product class descriptions.

A.2 Minimum set of functions defining Generic NFV-MANO class

A generic NFV-MANO product class is a class of products that all implement a common set of ETSI-defined functionalities. This common set is defined to be the list of functions contained in pertinent ETSI specifications.

A.3 Generic model

A.3.1 Generic NFV-MANO product model overview

Figure A.3-1 depicts the components of a generic NFV-MANO product model at a high level. These components are further described from clause A.3.2 to clause A.3.5.

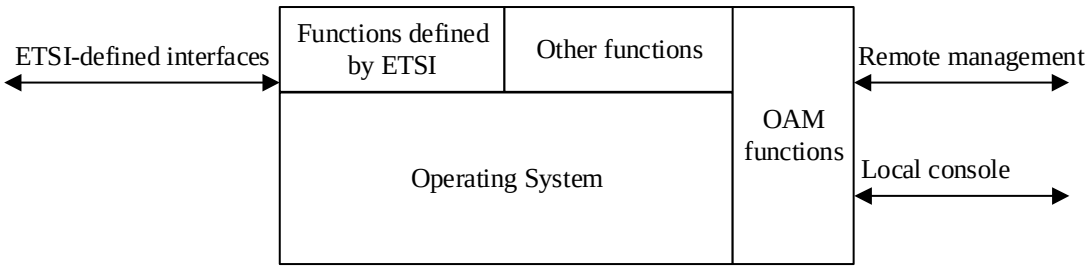

Figure A.3-1: Generic NFV-MANO product model

A.3.2 Functions defined by ETSI

A generic NFV-MANO product will, in many cases, implement ETSI-defined functions from various releases of pertinent ETSI specifications. Vendors are, to a large extent, free to select the features implemented in their NFV-MANO products.

A.3.3 Other functions

A generic NFV-MANO product will also contain functionality not or not fully covered in ETSI specifications.

Examples include, but are not limited to, local or remote management functions.

A.3.4 Operating System (OS)

The present document assumes that the generic NFV-MANO product is implemented on dedicated or shared hardware that requires an operating system to run.

A.3.5 Interfaces

There are two types of logical interfaces defined for the generic NFV-MANO product:

- remote logical interfaces; and
- local logical interfaces.

A **remote logical interface** is an interface which can be used to communicate with the generic NFV-MANO product from another network node.

A **local logical interface** is an interface that can be used only via physical connection to the generic NFV-MANO product. That is, the connection requires physical access to the generic NFV-MANO product.

Annex B (informative): Generic NFV-MANO assets and threats

B.1 Introduction

The present annex contains assets and threats that are believed to apply to more than one network product.

B.2 Generic critical assets

The critical assets of generic NFV-MANO product to be protected are:

- user account data and credentials (e.g. passwords);
- log data;
- configuration data, e.g. generic NFV-MANO product's IP address, ports, VPN ID, Management Objects (e.g. user group, command group), etc.;
- Operating System (OS) i.e. the files that make up the OS and its processes (code and data);
- generic NFV-MANO product Application;
- sufficient processing capacity: that processing powers are not consumed close to limits;
- the interfaces of generic NFV-MANO product to be protected and which are within SECAM scope: for example:
  - console interface, for local access: local interface on NFVO;
  - OAM interface, for remote access: interface between NFVO and OAM system;
- generic NFV-MANO product Software: binary code or executable code.

B.3 Generic threats

B.3.1 Generic threats format

Threats are described using the following format:

- *Threat Name*:
- *Threat Category*:
- *Threat Description*:
- *Threatened Asset*:

B.3.2 Threats relating to ETSI-defined interfaces and functions

B.3.2.1 Weak cryptographic algorithms

- *Threat name*: Weak cryptographic algorithms.
- *Threat Category*: Information Disclosure.

- *Threat Description:* Usage of weak cryptographic algorithms for stored or transmitted sensitive information/data can expose them to be disclosed and eventually tampered.
- *Threatened Asset:* all critical asset in the generic NFV-MANO product as listed in clause B.2.

B.3.3 Spoofing identity

B.3.3.1 Default Accounts

The threat in clause 5.3.3.1 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.3.2 Weak Password Policies

The threat in clause 5.3.3.2 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.3.3 Password peek

The threat in clause 5.3.3.3 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.3.4 Direct Root Access

The threat in clause 5.3.3.4 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.3.5 IP Spoofing

The threat in clause 5.3.3.5 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product. However, the objective of unauthorized access is a generic NFV-MANO product, not a computer

B.3.3.6 Malware

The threat in clause 5.3.3.6 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.3.7 Eavesdropping

The threat in clause 5.3.3.7 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.4 Tampering

B.3.4.1 Software Tampering

The threat in clause 5.3.4.1 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.4.2 Ownership File Misuse

The threat in clause 5.3.4.2 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.4.3 External Device Boot

For generic NFV-MANO product, there is no hardware. This is different from external device boot of generic NFV-MANO product described in clause 5.3.4.3 of ETSI TR 133 926 [i.1]. The threat is described as follows:

- *Threat name*: generic NFV-MANO product boot tampering.
- *Threat Category*: Tampering.

- *Threat Description:* the generic NFV-MANO product bootloader may be maliciously tampered by an attacker, e.g. the attacker tampers the bootloader of generic NFV-MANO product through a malicious virtualisation layer.
- *Threatened Asset:* guest operating system.

B.3.4.4 Log Tampering

The threat in clause 5.3.4.4 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.4.5 OAM Traffic Tampering

The threat in clause 5.3.4.5 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.4.6 File Write Permissions Abuse

The threat in clause 5.3.4.6 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.4.7 User Session Tampering

The threat in clause 5.3.4.7 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.5 Repudiation

B.3.5.1 Lack of User Activity Trace

The threat in clause 5.3.5.1 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6 Information disclosure

B.3.6.1 Poor key generation

The threat in clause 5.3.6.1 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.2 Poor key management

The threat in clause 5.3.6.2 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.3 Weak cryptographic algorithms

The threat in clause 5.3.6.3 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.4 Insecure Data Storage

The threat in clause 5.3.6.4 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.5 System Fingerprinting

The threat in clause 5.3.6.5 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.6 Malware

The threat in clause 5.3.6.6 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.7 Personal Identification Information Violation

The threat in clause 5.3.6.7 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.8 Insecure Default Configuration

The threat in clause 5.3.6.8 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.9 File/Directory Read Permissions Misuse

The threat in clause 5.3.6.9 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.10 Insecure Network Services

The threat in clause 5.3.6.10 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.11 Unnecessary Services

The threat in clause 5.3.6.11 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.12 Log Disclosure

The threat in clause 5.3.6.12 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.13 Unnecessary Applications

The threat in clause 5.3.6.13 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.14 Eavesdropping

The threat in clause 5.3.6.14 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.6.15 Security threat caused by lack of generic NFV-MANO product traffic isolation

The threat in clause 5.3.6.15 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.7 Denial of service

B.3.7.1 Compromised/Misbehaving User Equipments

The threat in clause 5.3.7.1 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.7.2 Implementation Flaw

The threat in clause 5.3.7.2 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.7.3 Insecure Network Services

The threat in clause 5.3.7.3 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.7.4 Human Error

The threat in clause 5.3.7.4 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8 Elevation of privilege

B.3.8.1 Misuse by authorized users

The threat in clause 5.3.8.1 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8.2 Over-Privileged Processes/Services

The threat in clause 5.3.8.2 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8.3 Folder Write Permission Abuse

The threat in clause 5.3.8.3 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8.4 Root-Owned File Write Permission Abuse

The threat in clause 5.3.8.4 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8.5 High-Privileged Files

The threat in clause 5.3.8.5 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8.6 Insecure Network Services

The threat in clause 5.3.8.6 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

B.3.8.7 Elevation of Privilege via Unnecessary Network Services

The threat in clause 5.3.8.7 of ETSI TR 133 926 [i.1] is generic, so it also applies to generic NFV-MANO product.

Annex C (informative): Change History

Date	Version	Information about changes
December 2022	V0.0.1	First draft as baseline.
March 2023	V0.0.1	Revised based on WI clarification.
June 2023	V0.0.2	Implementation of the following contribution accepted during the SEC#224 meeting NFVSEC(23)000041r2_SEC028_Protection_at_the_transport_layer and the following contribution accepted during NFVSEC#230-at NFV#42 NFVSEC(23)000125_Exceptions_list_proposal_for_MANO_SCAS.
August 2023	V0.0.3	Implementation of the following contribution accepted during the SEC#236 meeting NFVSEC(23)000184_cleanup_and_propose_stable_draft_for_SEC028.
September 2023	V0.0.4	Implementation of the following contribution accepted during the SEC#238 meeting NFVSEC(23)000191_NFVSEC028ed451_Protection_at_the_transport_layer and NFVSEC(23)000192_Revisions_to_the_OS_description.
November 2023	V4.5.1	First published version.
January 2024	V5.0.1	Incorporating contributions NFVSEC(23)000213r2 and NFVSEC(24)000001r1.

History

Document history		
V5.1.1	May 2024	Publication