**3GPP TSG-SA3 Meeting #100bis-e *S3-202561***

**e-meeting, 12 -16 October 2020** Revision of S3-20xxxx

**Source: China Mobile**

**Title: Adding hardening requirements for GVNP of type 1**

**Document for: Approval**

**Agenda Item: 2.2**

# 1 Decision/action requested

***This contribution adds hardening requirements for GVNP of type 1 into clause 5.2.5.5.8.***

# 2 References

[X] 3GPP TR 33.117: "Catalogue of general security assurance requirements"

# 3 Rationale

Compared to the physical network products, GVNP of type 1 has not hardware, but has infrastructure management traffic rather than O&M traffic, control plane traffic and data plane traffic etc. The hardening requirements shall consider how to reduce the exposure for GVNP of type 1. This contribution proposes some hardening requirements and related test cases for GVNP of type 1. We propose to add these hardening requirements and related test cases into clause 5.2.5.5.8.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.5.5.8 Security requirements and related test cases to Hardening for GVNP of type 1

5.2.5.5.8.1 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 related to general hardening requirements (i.e. technical baseline), the operating system, web server, network devices will be described in the following clauses.

5.2.5.5.8.2 Technical Baseline

5.2.5.5.8.2.1 No unnecessary or insecure services / protocols

All text from TS 33.117 [4], clause 4.3.2.1 applies to GVNP of type 1.

5.2.5.5.8.2.2 Restricted reachability of services

All text from TS 33.117 [4], clause 4.3.2.2 applies to GVNP of type 1.

5.2.5.5.8.2.3 No unused software

All text from TS 33.117 [4], clause 4.3.2.3 applies to GVNP of type 1.

5.2.5.5.8.2.4 No unused functions

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [4] clause 4.3.2.4 applies to GVNP of type 1, except the requirements and testing on hardware functions.

5.2.5.5.8.2.5 No unsupported components

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [4] clause 4.3.2.5 applies to GVNP of type 1, except the requirements and testing on hardware components.

5.2.5.5.8.2.6 Remote login restrictions for privileged users

All text from TS 33.117 [4], clause 4.3.2.6 applies to GVNP of type 1.

5.2.5.5.8.2.7 Filesystem Authorization privileges

All text from TS 33.117 [4], clause 4.3.2.7 applies to GVNP of type 1.

5.2.5.5.8.3 Operating System

Guest OS provided by the vendors is generally based on Linux. All hardening renquiremnets of OS in clause 4.3.3 of TS 33.117 [4] are general requirements and can be applied to GVNP of type 1.Editor’s Note: Hardening requirements for Guest OS not based on Linux are FFS.

5.2.5.5.8.4 Web Severs

All hardening renquiremnets of Web Servers in clause 4.3.4 of TS 33.117 [4] are general requirements and the same for both the virtualised network product and the physical network product. So, all text from TS 33.117 [4] , clause 4.3.4 applies to GVNP of type 1.

5.2.5.5.8.5 Virtualized Network Products

5.2.5.5.8.5.1 Traffic separation

All text from TS 33.117 [4], clause 4.3.5.1 applies to GVNP of type 1, except for the supporting physical separation of traffic belonging to different network domains.

5.2.5.5.8.5.2 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 VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated.

Editor’s Note: Threat analysis for this requirement and corresponding the test cases is to be added. A figure illustrating the scenario needs to be added.

5.2.5.5.8.5.3 Separation of infrastructure management traffic and VNF traffic related to service

*Requirement Name*: infrastructure management traffic and VNF service traffic separation

*Requirement Description*:

In addition to the traffic related to service (i.e O&M traffic, control plane traffic and/or data plane traffic), a VNF has the infrastructure management traffic which is for managing the virtualized resource of the VNF provided by the virtualization layer. The virtualized network product shall support logical separation of traffic between the infrastructure management traffic and the VNF service traffic.

*Threat Reference*: 5.2.4.2.2.7.15 Security threat caused by lack of GVNP traffic isolation

*Test case*:

**Test Name:** TC\_TRAFFIC\_SEPARATION\_INFRASTRUCTURE\_SERVICE

**Purpose:**

To test whether infrastructure management traffic is separated from VNF service traffic.

**Procedure and execution steps:**

**Pre-Condition:**

Test environment with a VNF and a virtualisation layer (or simulated virtualisation layer).

**Execution Steps**

**Execute the following steps:**

1. The tester checks whether the infrastructure management traffic and VNF service traffic are separated according to the vendor’s documents.

2. The tester checks whether the VNF rejects infrastructure management traffic on all VNF service related interfaces.

3. The tester checks whether the VNF rejects VNF service traffic on all infrastructure management interfaces.

**Expected Results:**

In the step 1, the infrastructure management traffic and VNF service traffic are separated according to the vendor’s documents. In the step 2 and step 3, the VNF rejects the traffic on the inspected interfaces.

**Expected format of evidence:**

A PASS or FAIL.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*