**3GPP TSG-SA3 Meeting #101-e *S3-203132***

**e-meeting, 9 -20 Novenber 2020** Revision of S3-20xxxx

**Source: China Mobile**

**Title: Adding basic vulnerability testing requirements for GVNP**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution adds basic vulnerability testing requirements for GVNP 5.z.***

# 2 References

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

# 3 Rationale

Compared to the physical network products, the GVNP’s operating system, software etc. may contain vulnerabilities and some ports (e.g. 8080, 443, 22) need to be opened for services. The current FOSS and COTS security testing tools already support vulnerability and port scanning for the virtualized network products.

The target of robustness and fuzz testing are the protocol stacks (e.g. diameter stack) rather than the applications. The protocol stacks supported by NF are the same for both virtualized and physical network products. So, all text from TS 33.117, clause 4.4 applied to all types of GVNPs. This contribution adds basic vulnerability testing requirements for GVNP 5.z.

# 4 Detailed proposal

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

## 5.z Basic vulnerability testing requirements for GVNP

### 5.z.1 Introduction

The basic vulnerability testing activeties such as Port Scanning, Vulnerability Scanner by the use of vulnerability scanners are the generic mechanisms to detect the exposures and vulnerabilities of both for the physical network products and the virtualized network products. Currently, the security testing tools already support vulnerability and port scanning for the virtualized network products. So, the requirements of port scanning and vulnerability scanning in clause 4.4 of the TR 33.117 apply to GVNP.

The target of robustness and fuzz testing are the protocol stacks (e.g. http stack) rather than the applications. The protocol stacks supported by the NF are the same for both of virtualized and physical network products. So, all text from TS 33.117 [4], clause 4.4 applied to all types of GVNPs.

### Such general requirement should be applied to fit different kinds of implementations. For example, for GVNP of type 1, as it contains VNF, BVT is applied. For GVNP of type 2, BVT can be applied for its VNF part. If its virtualization layer part has host OS, BVT is also applied for its virtualization part. For GVNP of type 3, BVT can be applied for its VNF part, virtualization layer part if host OS is exists, and hardware part if SNMP or similar protocol exists. All these are based on detailed implementation of specific GVNP. 5.z.2 Port Scanning

All text from TS 33.117 [4], clause 4.4.2 applied to all types of GVNPs.

### 5.z.3 Vulnerability Scanning

All text from TS 33.117 [4], clause 4.4.3 applied to all types of GVNPs.

### 5.z.4 Robustness and Fuzz testing

All text from TS 33.117 [4], clause 4.4.4 applied to all types of GVNPs.

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