**3GPP TSG-SA3 Meeting #101-e *S3-20xxxx***

**e-meeting, 9th – 20th November 2020** Revision of S3-203166

**Source: Nokia, Nokia Shanghai Bell**

**Title: SCAS VNP: VM Escape and Hypervisor Escape**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***SA3 is kindly asked to approve the proposed changes in TR 33.818 v0.8.0.***

# 2 References

[1] 3GPP TR 33.818 v0.8.0 Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS); for 3GPP virtualized network products

# 3 Rationale

In current TR 33.818 v0.8.0 [1], the analysis of threats on the interface between virtualisation layer and VNF for GVNP type 2 is not quite complete. This pCR proposes additional text for the threat analysis.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.4.3.2.3 Threats relating to ETSI-defined interfaces

In addition to threats described in clause 5.2.4.2.2.3, GVNP of type 2 also has following threats relating to ETSI-defined interfaces[11]:

- The threats on interface between virtualisation layer and hardware: an attacker can utilize the vulnerabilities of hardware (e.g. Meltdown and Spectre of CPU in host) to attack virtualisation layer and/or VNFs through this interface, resulting in information disclosure or DoS etc.

- The threats on interface between virtualisation layer and VIM: an attacker can tamper the specific assignment of virtualized resources to cause resource assignment errors or an attacker can intercept virtualized resources state information leading to information disclosure.

- The threats on interface between virtualisation layer and VNF: an attacker can utilize the vulnerability of a 3GPP VNF to compromise the VNF. If one of the instances of a 3GPP VNF is compromised, other instances of the 3GPP VNF could be compromised in the same way by the attacker by executing a VM escape or hypervisor escape from the compromised instance.

NOTE: VM escape is a security exploit that an attacker runs code on a VM allowing the Guest OS of the VM to break out and interact directly with the host OS. Such an exploit enables the attacker to gain access to the hypervisor and all its created VMs. Hypervisor escape is a security exploit that an attacker is able tunnel through the virtualisation layer from an attacked VNF to any other VNF. VM escape is considered more likely than hypervisor escape, and hypervisor escape is considered more catastrophic than VM escape.

NOTE: the threats on the interface between 3GPP VNF and virtualisation layer only apply when VNF is decoupled from virtualisation layer.

Editor’s note: More threats described in 3GPP TR 33.848[9] or/and ETSI specifications are to be added if identified as related to the above two interfaces.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*