**3GPP TSG-SA3 Meeting #115 *S3-240775***

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.927** | **CR** | **0002** | **rev** |  | **Current version:** | **18.1.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Add VM traffic isolation security threat to TR 33.927 3GPP virtualized network product classes | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China Mobile | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | VNP\_SECAM\_SCAS | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | For the Security threat caused by lack of GVNP traffic isolation, the current version refers to “the threat in clause 5.3.6.15 of TR 33.926”, which mainly mentions the threat of lacking isolation for signalling traffic. For GVNP, the malicious traffic traffic between VMs can cause unauthorized access or attack. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add VM traffic isolation security threat | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The threat caused by applying virtualization technology is not fully considered. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.2.7.15 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

5.3.2.7.15 Security threat caused by lack of GVNP traffic isolation

The threat in clause 5.3.6.15 of TR 33.926 [2] applies to GVNP of type 1.

Different from traditional physical network products, as GVNP provides abundant computing, storage and network resources for users. With Virtualization, traditional physical network security appliances can not be used to secure virtual networks between VM on the same physical server. Additionnal threats are analysed as follows:

*- Threat name*: Security threat caused by lack of GVNP traffic isolation

*- Threat Category*: Information Disclosure.

*- Threat Description*: Virtual network has invisible traffic between VMs on the same physical server, which is not protected by the traditional network security monitoring means. Flaws such as incomplete isolation of virtual machine resources and the difficulty of monitoring traffic between virtual machines can lead to unauthorized access to VMs and mutual attacks between VMs.

*- Threatened Asset*: Any sensitive data in transit between VMs on the same physical server.

\*\*\* END CHANGES \*\*\*