**3GPP TSG-SA3 Meeting #114e *ad-hoc draft\_S3-240047-r1***

Electronic meeting, online, 22 - 26 January 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0162** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *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:***  | Addressing subjective comments from GSMA and comments in BSI AIS-N2to 4.2.4.1.2.1 |
|  |  |
| ***Source to WG:*** | Huawei; HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  SCAS\_5G\_Ph3 |  | ***Date:*** | 2024-01-22 |
|  |  |  |  |  |
| ***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 canbe 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:*** | GSMA commentted that expert knowledge is subjective and said one of the solution is to remove the sentence.The change is proposed to reflect the addition from clause 2.3.1.23 of AIS\_N2 document which is for NESAS CCS-GI. |
|  |  |
| ***Summary of change:*** | Replace the sentence “his expert knowledge of the operating system(s) used in the network product” by matches the vendor provided documentation.Add a new precondition. |
|  |  |
| ***Consequences if not approved:*** | misalignement with NESAS documents. |
|  |  |
| ***Clauses affected:*** | 4.2.4.1.2.1 |
|  |  |
|  | **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:*** |  |

 \*\*\*\*\*\*\*\*\*\*\*\*\* 1st of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

4.2.4.1.2.1 Authenticated Privilege Escalation only

*Requirement Name*: Authenticated Privilege Escalation only.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.. Implementation example: Disable insecure privilege escalation methods so that users are required to (re-)login directly into the account with the required permissions.

*Threat References*: TR 33.926 [4]

*Test Case*:

**Test Name**: TC\_OS\_PRIVILEGE

**Purpose:**

To ensure that privileged operating system functions shall not be used without successful authentication and authorization, and that violations of this requirement are documented and strictly limited in number and functionality.

**Procedure and execution steps:**

**Pre-Conditions:**

1. The vendor shall provide documentation of the operating system(s) used in the network product.

2. The vendor shall supply a list "A" of operating system functions which a system user can use to explicitly gain higher privileges, and how these functions are configured. Unix® example: sudo command and its configuration file /etc/sudoers or used Linux® capabilities.

3. The vendor shall supply a list "B" of operating system commands, GUI functions, and files which will execute specifically limited tasks automatically with higher privileges, even when used by a low-privileged user. List "B" shall also contain:

- configuration of these commands and GUI functions;

- owner and permission settings of files;

- justification for having the command, GUI function or file on the network product
Unix® example: root-owned files with SUID and SGID permissions or Linux® capabilities.

- capabilities of the aforementioned files.

NOTE: Linux® capabilities can provide a subset of root user privileges to a process rather than granting total root access. Some capabilities can be used for privilege escalation

**Execution Steps**

The tester is required to execute the following steps:

1. The tester logs into the network product and verifies that list "A" matches the vendor provided documentation.

2. The tester verifies that entries in the list "A" require successful authentication for all users without exception, on basis of the user name and at least one authentication attribute.

3. The tester logs into the network product and verifies that list "B" is accurate based on the vendor provided documentation mentioned in the pre-conditions in this clause. Unix® example: To list files with SUID and SGID permissions and Linux® capabilities, the following commands can be used:

SUID: find / -perm -4000 -type f -exec ls {} \; > suid\_files.txt

SGID: find / -perm -2000 -type f -exec ls {} \; > sgid\_files.txt

Capabilities: getcap -r / 2>/dev/null

4. The tester verifies that file entries in the list "B" do not have write permissions for anyone else than the owner.

5. The tester verifies that entries in the list "B" only allow execution of specifically limited tasks which are needed on this network product, based on the vendor provided documentation.

6. The tester logs into the network product and tests for every entry in the list "B" that it does not provide a means to execute arbitrary functions with administrator/root privileges, e.g. via a shell escape.

**Expected Results:**

1. The network product does not allow a user to gain administrator/root privileges from another user account without re-authentication.

2. If a network product provides functions and files which execute specifically limited tasks automatically with higher privileges, it ensures that these limits cannot be bypassed.

3. The system documentation about means for a user to gain administrator/root privileges from another user account accurately describes the network product.

**Expected format of evidence:**

A test report provided by the tester which will consist of the following information:

 - Documentation provided by the vendor: lists "A" and "B"

- Description of executed tests and commands

 - Relevant output (e.g. screenshot or terminal log)

 - Test result (passed or not passed)

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