**3GPP TSG- Meeting # *20-r1***

**, , -**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | External file system mount restrictions (TC\_EXTERNAL\_FILE\_SYSTEM \_MOUNT\_RESTRICTIONS) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Ph3 | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | |  |
|  | *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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Rewrite of test case so it is objective and meets the NESAS purpose. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding clarification on suitable privilege escalation method. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Text could be interpreted differently by different Test Labs, making it extremely difficult to be certain that all tests are being conducted such that the results would be the same, regardless of which Test Lab did the work. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.3.3.1.6 External file system mount restrictions | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 OF CHANGE \*\*\***

##### 4.3.3.1.6 External file system mount restrictions

*Requirement Name*: External file system mount restrictions

*Requirement Description*:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

Implementation example: In Linux® systems, administrators shall set the options nodev and nosuid in the /etc/fstab for all filesystems, which also have the "user" option.

NOTE: This requirement does not apply when the docker is used to mount file system.

*Test Case*:

**Test Name**: TC\_EXTERNAL\_FILE\_SYSTEM\_MOUNT\_RESTRICTIONS

**Purpose:**

Verify that OS-level restrictions are set properly for users that are allowed to mount external file systems (attached locally or via the network). This is to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

**Procedure and execution steps:**

**Pre-Condition:**

Tester has admin access to check and configure the external filesystem mount permissions in the OS.

Tester has username and password of a user in the network product that has external filesystem mount privileges.

**Execution Steps**

**Execute the following steps:**

1. The tester shall verify that OS-level restrictions are set properly in order to prevent privilege escalation due to the contents of the mounted file systems (e.g. In Linux® systems, administrators shall set the options nodev and nosuid in the /etc/fstab for all filesystems, which also have the "user" option). The tester checks that OS-level parameters are configured correctly on the system.

2. The tester mounts an external filesystem prepared by the tester with files exploiting privilege escalation methods (e.g. with writable SUID/GUID files).

3. The tester tries to gain privileged access to system by using a suitable privilege escalation method using the contents of the mounted file system and then confirms that privilege escalation doesn't happen.  
A suitable privilege escalation method is one that is effective, reliable, and does not introduce additional security vulnerabilities.

**Expected Results:**

The OS-level restrictions are set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

Any privilege escalation method used by the tester should be blocked.

**Expected format of evidence:**

Screenshot containing the configuration file showing that OS-level restrictions are set properly for users that are allowed to mount external file systems.

**\*\*\* END OF CHANGE \*\*\***