**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 -26 May 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HELP***](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 | **X** | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification of privilege verification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Federal Office for Information Security (BSI) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 2023-05-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | The execution steps only repeat the requirement description and do not contain any concrete task. For verifiability and reproducibility reasons, the execution steps should describe concrete tasks.  The execution steps do not test if the privileges of a web server get dropped to minimal privileges if the web server was started with system privileges.  The configuration that is used to transfer the execution of the web server from a user with system privileges to a user without system privileges should be provided as test evidence. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Rewrite the execution steps to ensure that the web server is configured with minimal privileges.  Add concrete test steps to actually verify the fulfilment of the requirements.  Add evidence for part of the configuration that shows how the privileges are dropped. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Different interpretations of the execution steps are possible. Therefore verifiability and reproducibility is not guaranteed.  It cannot be ensured that the web server runs with minimal privileges.  Insufficient verifiability and reproducibility due to missing evidences. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.3.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

4.3.4.2 No system privileges for web server

*Requirement Name*: No system privileges for web server.

*Requirement Description*:

No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

*Test Case*:

***Test Name*:** TC\_NO\_SYSTEM\_PRIVILEGES\_WEB\_SERVER

**Purpose:**

Verify that the Web server is not run under system privileges.

**Procedure and execution steps:**

**Pre-Conditions:**

- The tester has needed administrative privileges.

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured /script adapted in line with the Requirement Description.

**Execution Steps**

1. Check that no web server processes run with system privileges. Check that this is the case even for processes that may have been started by a user with system privileges.

a. Start the web server process as web server user and check process privileges.

b. Start the web server proves as with system privileges and check if process privileges get dropped.

2. Check in relevant system settings and web server configurations that a web server user is configured with minimal privileges and the web server is executable by that user.

**Expected Results:**

- There are no findings of processes that run with system privileges.

- System settings have been found correctly set to ensure that no processes will run with system privileges.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files / command line output and screen shots of test executions

- Part of web server and/or system configuration (plain text or screenshot) showing the configured user for the web server process

- Test result (Passed or not)

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