**3GPP TSG-SA3 Meeting #114-e *S3-240072-r2***

**Electronic meeting, online, -**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0175** | **rev** | **2** | **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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Updates to Section 4.3.6.2 of TS 33.117 for clarification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | IIT Bombay | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Ph3 | | | | |  | ***Date:*** | | | 2024-1-24 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Basic corrections to align TS 33.117 to address the feedback from GSMA NESAS group (S3-234423). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Few changes and additions to ensure test case has more clarification in Pre-conditions and execution steps, based on inputs from GSMA NESAS group. The proposed changes to be incorporated into ongoing development of Release 18 versions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear text in test case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.3.6.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

4.3.6.2 No code execution or inclusion of external resources by JSON parsers

*Requirement Name*: No code execution or inclusion of external resources by JSON parsers.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

Parsers used by Network Functions (NF) shall not execute JavaScript or any other code contained in JSON objects received on Service Based Interfaces (SBI). Further, these parsers shall not include any resources external to the received JSON object itself, such as files from the NF’s filesystem or other resources loaded externally.

*Threat References*: TR 33.926 [4], clause 6.3.2.1, JSON Parser Exploits

*Test Case*:

**Test Name:** TC\_JSON\_PARSER\_CODE\_EXEC\_INCL

**Purpose:**

NFs implementing SBI transfer application data serialized as JSON objects. When receiving such data, an NF parses this JSON representation and creates equivalent internal data structures. Since the contents of the JSON objects shall be considered untrusted, blindly executing code fragments or loading resources from a local path or Uniform Resource Identifier (URI) shall not be possible.

**Procedure and execution steps:**

**Pre-Conditions:**

- The tester has the privileges to log in the network product and to access to all system resources (e.g. log files)

- A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:

- all interfaces providing IP-based protocols;

- the available transport layer protocols on these interfaces;

- their open ports and associated services in the form of an OpenAPI3.0 interface specification;

- The tester has access to a Web Application Security (WAS) test tool that allows the tester to generate HTTP messages exploiting JSON parsers that do not prevent the above-mentioned scenarios of code execution and loading external resources. The test lab is expected to have sufficient expertise to recognize the level of effectiveness of the available tools.

- A network traffic analyser on the network product (e.g. TCPDUMP) or an external traffic analyser directly connected to the network product and on a tester machine is available.

**Execution Steps**

1. The tester uses a WAS test tool to generate HTTP requests (as described above in pre-conditions) towards the network product’s API endpoints via its Service Based Interfaces.

2. Using a network traffic analyser on the network product, e.g. TCPDUMP or an external traffic analyser directly connected to the network product, the tester verifies that no external resources get loaded during JSON parsing.

3. Depending on the actual JavaScript code in the HTTP message, the tester verifies that the network product does not execute any of the contained actions.

**Expected Results:**

- The NF does not load any resources external to the JSON object itself.

- The NF does not execute any JavaScript code contained in JSON objects.

**Expected format of evidence:**

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

- The used tool(s) name and version information

- Settings and configurations used

- The output log file of the chosen tool that displays the results (passed/failed).

- Screenshot

- Test result (Passed or not)

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