**3GPP TSG-SA3 Meeting #114-Ad Hoc-e *draft\_S3-240019\_r1***

**Online, , 22nd Jan 2024 - 26th Jan 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0147** | **rev** | **-** | **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:***  | Syn Flood Prevention [TC\_SYN\_FLOOD\_PREVENTION] |
|  |  |
| ***Source to WG:*** | Deutsche Telekom AG |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph3 |  | ***Date:*** | 2023-07-26 |
|  |  |  |  |  |
| ***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-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:*** | Rewrite the test execution to be more specific and other minor changes in the text. |
|  |  |
| ***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:*** | 4.3.3.1.4 |
|  |  |
|  | **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 \*\*\***

##### 4.3.3.1.4 SYN Flood Prevention

*Requirement Name:* Syn Flood Prevention

*Requirement Description:*

The network product shall support a mechanism to prevent Syn Flood attacks (e.g. implement the TCP Syn Cookie technique in the TCP stack by setting net.ipv4.tcp\_syncookies = 1 in the linux sysctl.conf file). This feature shall be enabled by default.

*Test Case:*

**Test Name**: TC\_SYN\_FLOOD\_PREVENTION

**Purpose:**

Verify that the Network Product supports a Syn Flood Prevention technique.

**Procedure and execution steps:**

**Pre-Conditions:**

- Vendor documentation describing the SYN flood attack prevention mechanism or setting and where to check for them.

- The Network Product is listening on a TCP port on one of its interfaces.

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

- A host is connected to the Network Product interface and it is equipped with a tool able to reproduce a Syn Flood attack (e.g. nmap or hping)

**Execution Steps**

1. The tester verifies the prevention mechanism or setting described in the vendor documentation.
2. The tester checks in the product documentation the link speed supported by the DUT in bytes (L).
3. The tester choose a size packet for the attack in bytes (S)
4. Based on L and S, the tester calculated the amount of *packets per second* (P) to use with this formula:

P = L / S

5. The tester configures the tool to send the number of packets calculated in step 4 of TCP Syn packets against the Network Product (e.g. hping3 -i <waiting time between each packet> -S -p <TCP port> -d <Data Size> -c <Number of packets> < Network Product IP>)

6. The tester verifies that the Network Product is still functioning as expected, its services are still accessible and responsive to typical service function requests, and the memory or CPU usage does not exceed acceptable thresholds. Additionally, the tester confirms there are no crashes or deadlocks.

 a. While the SYN Flood attack is ongoing.

 b. After the SYN Flood attack was executed.

**Expected Results:**

The Network Product does not become inoperative.

**Expected format of evidence:**

- Executed commands or script used for the SYN flood attack.

- Part of the configuration (plaintext or screenshot) showing the prevention mechanism or setting.

- A Pass/Fail result provided by the tester.

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