**3GPP TSG-SA3 Meeting #100e *S3-201761***

**e-meeting, 17 -28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | **Draft CR** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Threat analysis on NAS based redirection from 5GS to EPS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei;Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS | | | | |  | ***Date:*** | | | 17-08-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | R-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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | If the Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC is not protected, the attacker can modify the cause and the UE will try to connect to the EPS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add a new threat analysis to 33.926 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The threat cannot be well identified and the test on it cannot find its threat reference. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | K.2.X(new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### K.2.X NAS based redirection from 5GS to EPS in 5G CIoT

*- Threat name:* NAS based redirection from 5GS to EPS

*- Threat Category*: Denial of Service, Information disclosure.

*- Threat Description*: In NAS based redirection from 5GS to EPS in 5G CIoT , , when a UE initiates registration procedure with the AMF, the AMF may redirect the UE from 5GC to EPC with a Registration Reject message sent to the UE, and if the Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC is not protected, the attacker can modify the cause and the UE will try to connect to the EPS. This will lead to a bidding down attack to the UE.

*- Threatened Asset*: Sufficient Processing Capability, N1 interface, Mobility Management data .

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