**3GPP TSG-SA3 Meeting #101-e *S3-20xxxx***

**e-meeting, 9th – 20th November 2020 *revision of S3-203115***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DraftCR** | **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:***  | Updated Threat Analysis of Incorrect Verification of Access Tokens  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eSCAS\_5G  |  | ***Date:*** | 30-10-2020 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | The definition of access token claims was updated in TS 29.510 R16.Therefore, it is proposed to update the threat analysis of Incorrect Verification of Access Tokens in TR 33.926 R17 accordingly. |
|  |  |
| ***Summary of change:*** | Updated the threat analysis of Incorrect Verification of Access Tokens in clause 6.3.3.1 of TR 33.926 R17. |
|  |  |
| ***Consequences if not approved:*** | Insufficient threat anslysis for the purpose of the corresponding test case updated in TS 33.117 R17. |
|  |  |
| ***Clauses affected:*** | 6.3.3.1 |
|  |  |
|  | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.3.3.1 Elevation of privilege via incorrect verification of access tokens

- *Threat name*: Incorrect Verification of Access Tokens.

- *Threat category*: Elevation of Privilege, Information Disclosure, Denial of Service.

- *Threat Description*: there are following threats if the generic NF cannot correctly verify the access tokens:

- An access token may be tampered so that an attacker can arbitrarily access any services from any NF service providers within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services of any slices provided by the NF producer instances (excluded from the list of NSSAIs or the list NSI IDs) within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services provided by the NF producer instances outside the NF Set which it is allowed to access within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the disallowed resources or conduct disallowed actions on the resources for the services provided by a NF service provider within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can block service access by replacing the granted services/NF service providers with unavailable services/NF service providers, which leads to denial of service.

- An expired access token can be replayed so that an attack can access the services which may no longer be allowed by the NF service provider, which leads to elevation of privilege and consequently information disclosure.

*- Threatened Asset:* NF API data, NF Application, Sufficient processing capacity.

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