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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | 17.6.0 |  |
|  | | | | | | | | |
| *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 |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Threat reference for incorrectly encoded UE 5G security capabilities on the AMF NG interface | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Federal Office for Information Security (BSI) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 2023-05-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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 possibility of incorrectly encoded UE 5G security capabilities on the AMF NG interface is not covered by a threat reference yet. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added threat reference describing the threat associated with incorrectly encoded UE 5G security capabilities on the NG interface | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | In the worst case, the AMF implements an incorrect encoding function for the security algorithms used for AS security, resulting in incorrectly negotiated security algorithms on the air interface. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | | **X** |  | Test specifications | | | | TS 33.512 CR 0023.. | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

K.2.6.2 Invalid encoding of UE 5G security capabilities on the NG interface

- *Threat name:* Invalid encoding of UE 5G security capabilities on the NG interface

*- Threat Category:* Tampering of data, Information Disclosure

*- Threat Description:* A flawed AMF implementation that incorrectly encodes the UE 5G security capabilities from the initial UE registration request to the corresponding Context Setup Request message on the NG interface will pose a risk to the AS user plane and control plane. It should be noted that encoding from the NAS to the NGAP protocol in this case is not a one-to-one copy of the UE 5G security capabilities but must consider the specifics of the NGAP protocol. Specifically, four bits are available to the encoder at the NAS layer for NIA0, NIA1, NIA2, NIA3, while only three bits are available at the NGAP layer for these four algorithms. If the algorithms are not transferred correctly to the gNB/ng-eNB due to an incorrect implementation of the AMF, the RAN node will misinterpret the algorithm list, resulting in the selection of an incorrect security algorithm on the AS. In the end, this may result in the selection of an insecure (e.g. null) algorithm letting an attacker easily intercept or manipulate control plane data and user plane data, leading to information disclosure.

*- Threatened Asset:* User account data and credentials, Mobility Management data

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