FGT5021 Tunnel ID uniqueness failure

Description: An adversary controlling a user-plane function (gNB or UPF) may disrupt user traffic by assigning the new traffic a TEID already in use.

The Tunnel Identifier, TEID, is part of the Core Network Tunnel information and is assigned locally by the UPF and also by the gNB/ng-eNB for user plane routing for each UE served. The failure to guarantee the uniqueness of the TEID for a PDU session results in interruption of the routing of the user traffic. It also creates charging errors. If multiple PDU sessions were to share the same TEID at the same time, the counts for the network usage of a single PDU session will be in fact the counts for the network usage of multiple sessions, creating charging errors.

Rogue or erroneous configuration/implementation in gNB or UPF can cause an existing TEID to be assigned to a new PDU session. This can also happen during EPS to 5GS handover or roaming.

Labelling:

* Sub-technique(s): none
* Applicable Tactics: Impact

Metadata:

* Architecture Segment: User plane
* Platforms: 5G Network
* Permissions Required: None.
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Rogue or misconfigured gNB or UPF | Rogue or wrong configuration/implementation in gNB or UPF can cause existing TEID to be assigned to a new N3 reference point or PDU session. Clause J.2.2.2 of [1]  Duplicate TEID allocation can happen during EPS to 5GS handover or roaming.  Duplicate TEID can cause traffic disruption, charging issues and eavesdropping of legitimate subscriber data by adversary. Clause 5.8.2.3 of [2], clause 4.11.1.2.2 of [3] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM5094 | Ensure UPF and gNB/NG-eNB check for uniqueness for every new TEID they allocate locally. The newly assigned TEID must not have been in use in the past given certain amount of time (which should be set to the reasonable maximum tunnel lifetimes observed). |
| M1035 | Limit Access to Resource Over Network |
| M1047 | The UPF and g/eNB must keep a log of the TEIDs currently in use (which they assigned), and purge TEIDs once the tunnel is torn down. This log must be checked every time a new TEID is allocated. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Control or misconfiguration of gNB or UPF | Faulty implementation at gNB or UPF; or, control over gNB, and UPF |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |
| UE billing data | Billing data of legitimate UE |
| UE data interruption | UE’s reception of its data is disrupted. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | Packet inspection over the N3 interface. If two packets are seen to have the same TEID on the RAN to UPF interface, then it can be verified that they indeed belong to the same UE. It may be difficult to detect as it is per UE and per PDU session. |
| FGDS5003 | Charging system reports anomaly of subscriber CDRs. Periodic CDR audits can detect anomaly. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
| UE data disruption | UE user plane data gets disrupted |
| Incorrect charging | Incorrect subscribers' charging records are generated |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TR 33.926 “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”. | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3002 |
| 3GPP TS 23.501 “System architecture for the 5G System (5GS)”. | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144 |
| 3GPP TS 23.502, “Procedures for the 5G System (5GS); Stage 2 (Release 17)”, Technical Specification, v17.4.0, March 2022. | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

Background info:

