FGT5023 Charging fraud via NF control

Description: An adversary controlling a control plane network function (NF) may manipulate signaling or parameters to achieve charging/billing fraud where victim is UE or operator itself.

There are multiple procedures to support this adversarial behavior, and they depend on the NF that is compromised.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Fraud

Metadata:

* Architecture segment: Control-plane
* Platforms: 5G
* Access Type required:
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| SMF control | An adversary may control the SMF and assign the same SMF Charging Identifier to a device data flow as that of an existing victim device, to cause charging errors. Clause 5.1.4 & annex A.1 of [3].  The SMF can also pause charging for a given UE (even though not warranted), clause 4.4.4 of [4].  The SMF can also misreport 5G data used by a given UE. |
| PCF control | An adversary with control over the PCF can change policy so that UE is allowed to consume a service it was not subscribed to - but it will still be traceable to that UE. Clause 4.3.2 of [5]. |
| CHF control | An adversary with control over the CHF can ignore when PCF tells it that the spending limit for this subscriber has been reached or can ignore the SMS records from the SMSF (SMSF uses POST to put in data), or can ignore the 5G data the SMF reports ([3]) |
| NEF control or Application Function (AF) control exploiting weak NEF | Adversary on AF can attack a weak NEF. Or, the NEF can be compromised and conduct this attack without even an AF.  An AF can ask the NEF to change the “chargeable party” Clause 4.4.8 of [6], clause 4.4.4 of [7].  This is meant to support the AF being the chargeable party, but it’s imaginable how the AF can put a different AF as chargeable: it has to send the AF identifier, UE IP address, Sponsor ID, ASP ID, etc. even AppID. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM1506 | Periodic authentication / authorization of NF consumer e.g. SMF/PCF/CHF/NEF/AF by NRF will help detect rogue NFs. |
| FGM5094 | Rigorous checks of unique mapping of charging ID to PDU session (applicable to the SMF case). Management system (OSS/BSS) can generate alert for possible intervention. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE call/data records accuracy | Communications is denied |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5003 | Management system (OSS/BSS) checks uniqueness of charging ID for all new PDU sessions in non-roaming scenario and existing PDU sessions in handover and roaming scenario |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3rd Generation Partnership Project (3GPP) TR 33.926: “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, Technical Report, v17.3.0, December. 2021 | https://www.3gpp.org/DynaReport/33926.htm |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| 3GPP TS 32.255 “Telecommunication management; Charging management; 5G data connectivity domain charging; Stage 2” | https://www.3gpp.org/DynaReport/32255.htm |
| 3GPP TS 23.502 “Procedures for the 5G System (5GS)” | https://www.3gpp.org/DynaReport/23502.htm |
| 3GPP TS 23.503 “Policy and charging control framework for the 5G System (5GS); Stage 2” | https://www.3gpp.org/DynaReport/23503.htm |
| 3GPP TS 29.522 “5G System; Network Exposure Function Northbound APIs; Stage 3” | https://www.3gpp.org/DynaReport/29522.htm |
| 3GPP TS 29.122 “T8 reference point for Northbound APIs” | https://www.3gpp.org/DynaReport/29122.htm |

#doNotParse

Background info

(another reference, not public, is “Attacks by NF, M. Vanderveen, Nov. 2021)

IPlook has good diagram that can be basis of further reading:

<https://www.iplook.com/products/charging-function>

AGF receives SMF Nchf interface messages sent from SMF side, and carries out routing and forwarding of messages.

CDF collects billing messages, generates corresponding CDRs and sends them to CGF, which processes the CDRs and generates bill files for BOSS to collect through the file interface; meanwhile, CHF supports forwarding the billing request messages sent by SMF to BOSS and forwards BOSS responses to SMF.

