FGT5025 Falsify interconnect invoice

Description: An adversary in a roaming partner operator may send altered service usage for a given UE to the home operator of that UE.

Service fraud involves bypassing controls to gain access to services or resources which the adversary is not entitled to or charged for. This applies to 3G, 4G, 5G.

A dishonest roaming partner could falsify a UE service usage or route traffic through several partner networks inducing high termination fees to claim revenue in the form of service charges.

Labelling:

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

Metadata:

* Architecture segment: Roaming
* Platforms: 5G
* Access Type Required:
* Data Sources:
* Theoretical/Proof of Concept/Observed: Observed

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 |
| False charging | Signaling fraud may be undertaken by a partner operator, via false charging over international signaling interconnection. Clause 5.3 of [1]. Reference [2] mentions service fraud. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5503 | Employ home-routing instead of local breakout for user traffic (but this means more delay and lower quality of service) |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
|  |  |

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. |
| Operator revenue | Operator loses revenue |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5006 | Usage data analysis via AI/ML |
| FGDS5011 | Cross-check with subscriber services (if subscriber complains) |

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) |
|  |  |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, section 5.2, November 2019. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | https://arxiv.org/abs/2108.11206 |