FGT5010 Fraudulent AMF registration for UE in UDM

Description: An adversary in control of an AMF can register it in the UDM to serve a victim UE, in order to commit fraud or retrieve subscription data for UEs.

A UE can be legitimately de-registered or be caused to de-register. The UDM is the core network function that holds the current registration status and data of an UE. An adversary can exploit an incorrectly implemented UDM that does not update the authentication status of a UE upon a de-registration event, or the authentication status is incorrect. This flaw allows a malicious AMF to register itself in UDM (via Nudm\_UECM\_Registration Request API call). An adversary controlling an AMF can register that AMF Identifier in the UDM as the current AMF which is serving the UE.

This technique also applies to the SMF and SMSF (SMS Function), not just AMF, using the same API to the UDM.

Note: The references do not specify a next step/ultimate goal of this procedure (a 3GPP contribution mentions “stealing data from the UDM”; while “fraud” is hinted at in a GSMA document, so it is imaginable that an AMF may claim to serve the roaming UE when in fact it is not.)

For an adversary to achieve this, a UDM must be incorrectly implemented. The improperly configured UDM needs to be able to perform all of the basic functions, except that it does not mark a UE as de-registered when it powers off or is legitimately (or illegitimately) de-registered by the network.

Labelling:

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

Metadata:

* Architecture segment: Control-plane
* Platforms: 5G
* Access type required: admin
* 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 |
| Adversary registers an AMF it controls as the one serving a given UE that just de-registered | An adversary in control of an AMF registers that AMF in UDM (via Nudm\_UECM\_Registration Request) as serving a given UE that de-registered. If the UDM implementation does not update the authentication status of UEs as de-registered, it will accept that AMF. The adversary-controlled AMF can then potentially perform additional hostile actions such as fraud, claiming to have provided services (for roaming UEs), or obtaining other UE information from the UDM.  Note that the UDM does not communicate with the AMF based on OAuth tokens. Since AMF to UDM signaling is part of the key UE control plane, it may be that they have a permanent TLS connection (TBC) |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5013 | Implement security as per clause 6.1.9 of 3GPP TS 29.503, namely OAuth2.0 |
| FGM5014 | Cross check whether the requesting AMF is likely to be the one serving that UE now. Validate the expected geography of where UE actually may be, in comparison to the area that the requester AMF is supposed to serve. |
| FGM1506 | Periodic authentication / authorization of NF consumer e.g. AMF by NRF will help detect rogue AMFs.  Not currently in 3GPP/GSMA (TBC) specs, but it can be enhanced. It’s process management (OA&M) |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Faulty UDM implementation | If the UDM does not store the authentication status of a UE, or the authentication status is incorrect |

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. |
| UDM functionality | Functionality of this core network function |
| UE data | Data (user or control) belonging to the UE |
| UE location | Physical geo-location (course or fine) of the UE |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
|  |  |

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) |
| A rogue AMF could perform other hostile action on the victim UE | A rogue AMF could mount other attacks on the victim UE, but the UE is not currently registered on the network |

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, Dec. 2021, clause E.2.2.3 | https://www.3gpp.org/DynaReport/33926.htm |
| 3rd Generation Partnership Project (3GPP) TR 33.846,” Study on authentication enhancements in the 5G System (5GS)”, Technical Report, v17.0.0, December 2021, clause 5.3.1.2 | https://www.3gpp.org/DynaReport/33846.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 contribution (2019) | https://www.3gpp.org/ftp/Meetings\_3GPP\_SYNC/SA3/Inbox/Drafts/draft\_S3-194673\_was\_S3-194189\_Resolving%20the%20ENs%20in%20KI%233.1\_V3.docx |