FGT5020 Retrieve UE subscription data

Description: Adversary controlling a control plane network function (NF) may manipulate signaling to retrieve UE subscription information.

The AMF, SMF, NEF, SMSF and the UDM itself can use legitimate signaling to retrieve the subscription data of a given UE, assuming its SUPI is known. The subscription data is stored in the UDM or UDR.

The UE data in the UDM is referred to as the “Session Data Management Subscription data”, and it includes access and mobility subscription data, SMS subscription data, slice information (the UE’s NSSAIs), "supported features", serving PLMN ID. This threat consists of a compromised NF to ask the UDM for the data for a given SUPI or GPSI.

Labelling:

* Sub-technique(s):
* Applicable Tactics: Collection

Metadata:

* Architecture segment: Control-plane
* Platforms: 5G Core Network
* Access type required: admin
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| AMF retrieves subscription data from UDM. | An AMF can extract subscription data (including NSSAIs) for any given UE SUPI by asking the UDM (uses Nudm\_SDM\_Get service (SDM=SubscriberDataManagement)). The UDM does not check that that AMF is the one serving the UE, i.e. the AMF does not need to register itself first as serving the UE, via the Nudm\_UECM\_Registration Request. Table 5.2.3.1-1 of [1] |
| AMF in visited PLMN retrieves UE information during 5GS to EPC roaming. | A rogue AMF in visited PLMN can retrieve the UE’s sensitive information during 5GS to EPC roaming. AMF calls Nsmf\_PDUSession\_ContextRequest API to v/hSMF. SMF sends the UE SM context in response which can reveal the following UE information: SUPI, S-NSSAI, DNN, UE IP address etc. Clause 4.11.1.2.1 & Table 5.2.8.2.10-1 of [1] |
| SMF retrieves subscription data from UDM | The SMF can send to UDM a Nudm-sdm message and retrieve “Session mgmt subscription data”, i.e. DNN configuration for all network slices. |
| UDM can look up any UE (in UDR if one is employed). | The UDM can legitimately get UE subscription data from UDR. |
| SMSF retrieves UE subscription data from UDM | The SMSF can get the UE subscription data via Nudm\_sdm API. |
| NEF retrieves some of the UE subscription data from UDM. | The NEF can get the UE subscription data via Nudm\_sdm API. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| FGM5033 | Standard 5G enterprise/core network security functionality  E.g. Zero trust principles for OA&M. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| SUPI or GPSI | Adversary must know the SUPI or GPSI of victim UE |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UDM and subscriber/UE data | Subscriber data can be permanent (not updateable) or updateable (like the current serving PLMN, AMF etc) |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Monitor logs |

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** |
| 3rd Generation Partnership Project (3GPP) 23.502 “Procedures for the 5G System (5GS)”, March 2022. | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

Details are in the MITRE document “Attacks by Network Function”, M. Vanderveen, Nov. 2021.