FGT5012.006 NAS exploit

Description: An adversary may geolocate a UE using modified Non-Access Stratum (NAS) signaling.

NAS is signaling that is exchanged for registration and authentication between the UE and the Access and Mobility Function (AMF), via the gNB as a pass-through. Adversary uses a fake gNB to intercept, modify and/or replay NAS messages to probe for UE presence in a that cell, which leads to coarse location. The victim UE tried to connect to a nearby gNB, and adversary then lured UEs to connect to it (e.g., by increasing the transmit power of the fake gNB).

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: Discovery, Collection

Metadata:

* Architecture segment: RAN, Control plane
* Platforms: 5G Network
* Access type required: physical/gNB
* Data Sources: gNB radio signals (sent to all UEs to enable them to select gNB and connect) received and reported by UEs to the operator.
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Replay of NAS message | Adversary eavesdrops one NAS message from the legitimate network (the Auth\_Req (R, AUTN), or the NAS Security Mode Command (SMC)), then replays that NAS message whenever it wants to check whether the victim UE is nearby, since the type of error (or response, in the case of SMC) received from the responder indicates whether it's the victim UE or not. Thus, adversary can probe for UE’s presence in a that cell, which leads to coarse location data. See [1]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Control of fake gNB in the area where the victim UE may be located. | Adversary must install a fake gNB that it can control what messages it sends to UEs. |
| Control of fake UE in the NAS SMC attack. | Adversary must acquire a fake UE to achieve the NAS SMC attack. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE location | UE/Subscriber geographical location, coarse or fine-grained |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5002 | Operator standard means to detect presence of fake gNBs. gNB radio signals (sent to all UEs to enable them to select gNB and connect) are received and reported by UEs to the operator, who can then run cross checks with the signals that the UEs should have received if all gNBs nearby were legitimate. Clause 6.24 of [2] |

Post-Conditions

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

**References**

|  |  |
| --- | --- |
| **Name** | **URL** |
| X. Hu et.al. “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security”, IEEE Access, August 2019. | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8817957 |
| 3rd Generation Partnership Project (3GPP) TR 33.809: “Study on 5G security enhancements against False Base Stations (FBS)”, Technical Report, v0.18.0, February 2022. | https://www.3gpp.org/DynaReport/33809.htm |