FGT5012.002 Self Location Measurement

Description: An adversary may elicit location reports from UE that is bid down to less secure format or may passively observe location reports from UE employing null encryption.

An adversary may eavesdrop messages exchanged between the UE and the network, if encryption for the radio interface is not employed – either because the UE was downgraded from 5G to 4G, or because encryption was turned off by the network. These messages of interest contain location reports that the UE sends to the network upon (legitimate) request from the network.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Discovery, collection

Metadata:

* Architecture segment: RAN
* Platforms: 5G
* Access type required: RAN
* Data Sources: Transition to less secure format
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Self-location measurement | Victim UE is using a system with null encryption or is bid down to a less secure protocol. UE geolocation or geolocation measurement data is passively observed or, if bid down, actively ordered through illegitimate signaling. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5006 | Restrictive subscriber security profile. Do not use unencrypted systems. Set subscriber security profile to prohibit bidding down to less secure service. |
| FGM5096 | Disable location on UE device. This is only a partial mitigation because location parameters can still be available from UE. |
| M1041 | Avoid systems that employ null encryption. De-register when only NULL encryption is offered |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Permissive subscriber security profile OR system does not employ over-the-air encryption. | Subscriber security profile must allow bidding down to less secure format OR system does not employ over-the-air encryption. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| UE location | UE/Subscriber geographical location |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5010 | Subscriber transitions to less secure service. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subsequent attack | Geolocation can make electronic attack for degradation of service more effective, bidding down to defeat ID and traffic confidentiality more effective, and can expose subscriber to physical attack. |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| 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 |