FGT5015 Device database manipulation

Description: An adversary may compromise the Equipment Identity Register (EIR) and adds new equipment, modifies status (ok vs. stolen or prohibited) of mobile device.

EIR is an optional component (applicable to 3G, 4G, 5G) storing the status of a mobile equipment and optionally which Permanent Equipment Identifier (PEI) it is allowed to use. Compromising it can allow an adversary to modify status of devices (e.g. "stolen", "prohibited').

Note: Modifying the EIR does not affect the subscription data such as access to network slice, customer data, or allow fraudulent use of service.

Labelling:

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

Metadata:

* Architecture segment: Control plane, ICAM
* Platforms: 5G Network
* Access type required
* Data Sources: EIR logs
* 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 |
| EIR database compromise | Reference [1], DC-003, calls for the MNOs to employ an EIR. The rest of the attack is theoretical: an adversary may modify some of the entries in the EIR database, e.g. device status (stolen, etc.)  The AMF is the only function that checks the EIR based on PEI, upon UE registration (using the API N5g-eir\_EquipmentIdentityCheck\_Get). |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5020 | Secure EIR |

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. |
| Integrity of device database | Device databases should be kept from tampering. |
| User equipment status integrity | UE status should be kept accurate. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5009 | Difficult to detect unauthorized changes. Inspect logs of what changes were made and by whom in the EIR |

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** |
| GSM Association, “GSM Association Official Document FS.31, Baseline Security Controls.”, v2.0, Feb. 2020 | https://www.gsma.com/security/resources/fs-31-gsma-baseline-security-controls |