FGT5032 gNodeB Component Manipulation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: An adversary may compromise a component of gNodeB to affect radio network configuration.

The 3GPP standards assume that RAN functions are securely deployed, properly implemented, and do not contain components with malicious intent. If that assumption fails, malicious activity can take place.

The gNB is the termination point for encryption and integrity protection, if user plane traffic is sent in clear, it can potentially be exposed to an adversary controlling the gNodeB.

O-RAN Architecture puts network intelligence and management capability in SMO function, with Near Real Time Radio Intelligent Controller (RIC )and Non-Real Time RIC that can change the network behavior. It further allows xApps and rApps with standard interfaces to agents(if configured) outside the controlled network that can also read data and send configuration changes. A compromise of any of these components can potentially cause unintended changes to the network and expose user information.

3GPP does not dictate deployment models, so it is possible that improper security hardening and separation of networks between RAN VNF and Core VNF in the same Cloud or MEC may further allow lateral movements of adversary if a gNodeB component is compromised.

Labelling:

* Sub-techniques: FGT5032.001, FGT5032.002, FGT5032.003
* Applicable Tactics: Execution
* Platform(s): RAN
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:
* Architecture Segment: RAN

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known |  |

Mitigations

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

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| RAN Service Management and Orchestration | Configuration and data related to gNodeB |
| ORAN RIC | RIC and Configuration and data related to gNodeB |
| x-Apps | x-App and Configuration and data related to gNodeB, Realtime optimization data |
| r-Apps | r-App and Configuration and data related to gNodeB, non-Realtime optimization data |

Detection

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

Post-Conditions

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

References:

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

Notes: