FGT5032 gNodeB Component Manipulation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| July 19, 2023 | MV based on Jaemond’s | SMO function | Service Management and Orchestration framework |  |
| July 19, 2023 | MV based on Jaemond’s | Other highlights |  |  |
| July 19, 2023 | MV based on Jaemond’s | Removed hyphens from x-Apps, r-apps |  |  |

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 Service Management and Orchestration (SMO) framework, with Near-Real-Time Radio Intelligent Controller (Near-RT RIC) and Non-Real-Time RIC (Non-RT 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.

Unauthorized access to and manipulation of the gNB component can be carried out by a supply chain attack or as a result of malicious updates using operator’s management and deployment tools. Adversaries may also gain access by physically connecting to the device through an unsecured USB, serial, or COM port on the base station (or device hosting virtual CU/DU/RU/RIC), or by remotely logging in using SSH or Telnet if strong access control is not implemented.

In distributed deployment architectures, APIs present additional threat vectors that can be exploited by attackers. In shared RAN scenarios, the use of service configuration and management tools by multiple parties may increase the risk vectors.

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): O-RAN
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical
* 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 |
| xApps | xApp and Configuration and data related to gNodeB, Realtime optimization data |
| rApps | rApp and Configuration and data related to gNodeB, non-Realtime optimization data |

Detection

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

Post-Conditions

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

References:

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