FGT5032.002 gNodeB Component Manipulation: xApp

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

Description:

An adversary may compromise an xApp to affect the radio network configuration.

The O-RAN architecture includes the Radio Intelligence Controllers (RICs), which consists of the Non-Real-Time Radio Intelligent Controller (Non-RT RIC) and the Near-Real-Time Radio Intelligent Controller (Near-RT RIC), to optimize radio resource management of gNB components. The Non-RT RIC is embedded in the Service and Management Orchestration (SMO) framework and hosts rApps to provide policy-based guidance, machine learning model management and enrichment information to the Near-RT RIC function for the purpose of RAN optimization. The Near-RT RIC is a logical function that hosts xApps and enables near real-time control and optimization of the functions and resources of gNB components O-CU-CP, O-CU-UP and O-DU, steered via the policies and enrichment data provided from the Non-RT RIC.

xApps are applications designed to run on the Near-RT RIC to provide the desired RAN functionality. xApps are independent of the Near-RT RIC and may be provided by any third party. xApps on the Near-RT RIC can collect near real-time information from gNB components (O-CU-CP, O-CU-UP and O-DU) and influence behavior of those components thereby impacting 5G base station performance and delivery of services to a group of UEs or a single UE.

A compromise of an xApp (or through xApp Agent) can potentially lead to unauthorized changes in a CU or DU via E2 Interface.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: Execution

Metadata:

* Architecture Segment: RAN
* Platform(s): O-RAN
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples

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

Mitigations

|  |  |
| --- | --- |
| **MID** | **Use** |
|  |  |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| RAN Service Management and Orchestration | Configuration and date related to gNodeB |
| O-RAN RIC | RIC and Configuration and data related to gNodeB |
| xApps | xApp and Configuration and data related to gNodeB, Realtime optimization data |

Detection

|  |  |
| --- | --- |
| **DSID** | **Detects** |
|  |  |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| O-RAN.WG3.RICARCH-R003-v04.00 | https://orandownloadsweb.azurewebsites.net/specifications |
| ORAN.WG11.Threat-Model.O-R003-v06.00 | https://orandownloadsweb.azurewebsites.net/specifications |
| Federal Office of information Security, Study 5G RAN Risk Analysis | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?\_\_blob=publicationFile&v=5 |

#doNotParse