FGT5032.002 X-App

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-RT RIC and the Near-RT RIC, to optimize radio resource management of gNB components. The Non-RT RIC is embedded in the Service and Management Orchestration function 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 enables near real-time control and optimization of the functions and resources of gNB components CU-CP, CU-UP and 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 (CU-CP, CU-UP and 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-technique(s): N/A
* Applicable Tactics: Execution

Metadata:

* Architecture Segment: RAN
* Platforms: 5G Network
* Permissions required: None
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |

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 |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as: analyze logs. |

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 |
| O-RAN ALLIANCE, ‘Non-RT RIC: Functional Architecture’, O-RAN WG2: Non-real- time RAN Intelligent Controller and A1 Interface Workgroup, V01.01, Technical Report O-RAN.WG2.Non-RT-RIC-ARCH-TR-v01.01, Mar. 2021 | https://orandownloadsweb.azurewebsites.net/specifications |
| O-RAN ALLIANCE, ‘Non-RT RIC Architecture’, O-RAN WG2: Non-real- time RAN Intelligent Controller and A1 Interface Workgroup, Technical Specification O-RAN.WG2.Non-RT-RIC-ARCH-TS-v02.00, Mar. 2022 | https://orandownloadsweb.azurewebsites.net/specifications |
| Federal Office of Information Security, Study 5G RAN Risk Analysis, Accessed June 2022, section 5.1 | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?\_\_blob=publicationFile&v=5 |

#doNotParse

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated