FGT5032.001 Radio Intelligent Controller (RIC)

Description: An adversary may compromise a Radio Intelligent Controller (RIC) to affect radio network configuration.

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.

O-RAN RIC functions integrate and interact with xApps and rApps, which can bring information and instructions to the RIC from outside of the O-RAN architecture. A compromise of the RIC components (by any means) can potentially lead to unauthorized change in CU or DU via E2 Interface.

Labelling:

* Sub-technique(s):
* 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 |

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> |
| O-RAN ALLIANCE, ‘**O-RAN Security Threat Modeling and Remediation Analysis 3.0’**  , O-RAN SFG,, Technical Analysis O-RAN.SFG. O-RAN.SFG.Threat-Model -v03.00, July. 2022 | https://orandownloadsweb.azurewebsites.net/specifications |
| O-RAN ALLIANCE, ‘**O-RAN RIC Architecture**  ,ORAN WG3, Technical Specification O-RAN.WG3.RICARCH-v02.01  ,March 2022 | https://orandownloadsweb.azurewebsites.net/specifications |

Notes:

<https://www.ericsson.com/en/security/security-considerations-of-open-ran>

At present, the RIC has only high-level insights within a (radio resource) connection and does not have the ability to understand the connections between the same subscriber or other user equipments (UE). With no IMSI/IMEI correlation across connections (for both specific and multiple UEs), there is increased risk for false positive alarms/actions. For example, if a handset type causes many problems in a few cells, the RIC may not be able to understand and isolate that specific device issue and instead may falsely identify a systemic network issue.

* Limit risks associated with Near-Real-Time RIC, especially as related to control framework vs policy guidance capabilities and potential conflicts of xApps
* A1 Interface from Non-Real-Time RIC to Near-RT-RIC
* E2 Interface from Near-Real-Time RIC
* Near-RT RIC signaling conflicts with gNodeB
* Near-RT RIC xApps signaling can conflict
* xApp Root of Trust
* UE identification in the RIC

Each of the potential vulnerabilities is explained further in the subsections below. Further study is required to identify the best solutions to close these security risks.

#### **Near-RT RIC conflicts with gNodeB**

The Near-RT RIC is a logical entity that enables near-real-time control and optimization of a subset of the Radio Resource Management (RRM) functions performed by the gNB (CU-CP, CU-UP and/ or DU). The Near-RT RIC is composed of a software platform with applications, referred to as xApp, running on top. Each xApp can enable the Near-RT RIC to control one or multiple RRM functions. This is achieved by exchanging data between the xApps and the gNB over the E2 interface with control loops having timing in the order of 10ms to 1s. The RRM functions that can be controlled by the Near-RT RIC depend on the xApps and the capability of the RAN nodes exposed over the E2 interface. For example, the Near-RT RIC can control mobility and load balancing by exchanging information between a specific xApp and the CU-CP over E2. Another example is that the Near-RT RIC can control scheduling policies by exchanging information between another xApp and the DU. It is important to note that the RAN must be able to operate and provide services also without the Near-RT RIC or in case of Near-RT RIC failure.

The challenge with this definition of the Near-RT RIC is that there is no clear functional split between the Near-RT RIC and the gNB (CU-CP, CU-UP, DU). The functional split depends on the available xApps and the capabilities exposed by the gNB. This creates possible conflicts between the decisions taken by the Near-RT RIC and the gNB vendors that could lead to instability in the network, which introduces vulnerabilities that could be exploited by threat actors. For example, a threat actor can utilize a malicious xApp that intentionally triggers RRM decisions conflicting with the gNB internal decisions to create denial of service.