T1021: VNF Access Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| 8/10 | MV | Remote Services | Title should be changed | VNF Access Services |
|  |  |  |  |  |

Description: Adversary may use non-functional remote communication interfaces (SNMP/RCP, SSH) to change host configuration to enable host compromise.

In addition to the main functionality of the VNF itself, tenants may deploy additional network services with their containers. These services can be built into the VNF itself for example to allow monitoring or remote configuration. Moreover, tenants may unnecessarily install remote access services such as SSH into their containers to administer them remotely. If these network services are directly accessible over the Internet (or from another tenant of the CaaS), they provide an additional entry point for adversaries. For example, adversaries can try to guess access credentials or exploit known vulnerabilities in the network services. Once an adversary gained access to the container through these service, additional attacks become possible.

Labelling:

* Sub-techniques: none
* Applicable Tactics: lateral-movement, Discovery

Metadata:

* Architecture Segment: Impl-OA&M
* Platform(s): PNF, VNF Hosts
* Access type required: User, Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1032 | Use multi-factor authentication on remote service logons where possible. |
| M1018 | Limit the accounts that may use remote services. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs. |
|  |  |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Network functions | 5G or RAN Network functions including VNF and PNFs |
| Hosts, VMs, or Infrastructure elements | Virtualized 5G environment relies on underlying compute and SDN network elements which may be of interest to adversary |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0017 | Audit command logs |
| DS0028 | 5G NFs have defined interfaces, any other session establishment activity may be unauthorized. Monitor traffic patterns and session sources along with blocked/denied activity. |
| DS0029 | Monitor network traffic for expected and unexpected attempted and established connections |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| Fraunhofer AISEC, “Threat Analysis of Container-as-a-Service for Network Function “, Retrieved April 28 2022 | https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien\_TechReports/englisch/caas\_threat\_analysis\_wp.pdf |