T1021: VNF Access Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| 8/10 | MV | Remote Services | Title should be changed | VNF Access Services |
| 07/17/2023 | MV | Description paragraph is taken verbatim from Reference: | See new text. |  |
| 07/17/2023 | MV | SNMP/RCP, SSH | SNMP/RPC, SSH |  |

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

Cloud tenants may deploy additional network services with their containers in their containers along with the main functionality of the 5G Virtual Network Function (VNF). These services can be deployed as part of the VNF itself, since they allow for VNF monitoring or remote configuration. To this end, it is possible that possibly unsafe remote access services such as SSH may be deployed into the containers. If these network services are directly accessible over the Internet (or from another tenant of the CaaS), then they are vulnerable to intrusion attacks. For example, adversaries may attempt to guess access credentials or to exploit known vulnerabilities in the management services APIs. If successful, the adversary now can use the access to this container through these services for additional follow-on techniques.

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 |