T1599.503 Network Slice Application Resource Hijacking

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| July 20, 2023 | MV from AG’s comments | Capitalized mitigation network slice, critical asset completion |  |  |
|  |  |  |  |  |

Description: An adversary may use compromised container management SW (or account) in MANO domain to gain access to target VNFs and its resources for unauthorized access to resources/data of another slice in NFVI or resource exhaustion of target application resulting in denial of service.

Network Slice has a logical boundary, and within NS certain performance SLAs are guaranteed. A malicious software or adversarial actions in the NFV-MANO, modifies the affinity and anti-affinity rules for the constituents of VNFs/NSs in the catalogue or during an instantiation operation requested to the VIM, modifying the virtual resource isolation needs for these VNFs/NSs and enabling further attacks. This can result in placing adversary’s virtualized application on the same VM or container engine as target NF and allow for further attacks of container or VM escape or resource exhaustion.

Labelling:

* Sub-techniques: none
* Applicable Tactics: impact
* Platform(s):Slice
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:
* Architecture Segment: Arch-Slice, Impl-OA&M, Impl-Virtualization

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1026 | Least Privilege Access Control Policy - Access control policies should be granular to allow for optimal access to service requirements. |
| M1035 | Resource Policy enforcement -Create and enforce resource policy; policy can include SLA, quotas, QOS etc. |
| M1030 | Security and Trust zones -Security and trust zones can help isolate resources and can be mapped to business needs.  Micro and Nano segmentation- Implementing segmentation policy at granular level, network and compute resources can prevent some co-residency threats when mapped to SLAs, Users, and Resource policies.  Physical separation- Hardware, network, and point of presence can be separated to provide additional isolation. |
| FGM5505 | Hardware Mediated Execution Environment -Employ secure, hardware- based execution integrity as part of host/server design (M1041). |
| M1041 | Encryption can be used to protect data at rest and in transit |
| FGM5506 | Use of Network Slice Templates -Use of templates for network slicing can enforce baseline security and isolation requirements. These templates can be created for networks, compute and 5G slice functions deployments. |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| NFVI | NFVI includes orchestrators, network managers, and network elements |
| VNFs | 5G Core, RAN and Non-SBI functions, virtual resources supporting VNF |
| Slice Control and User Plane data | Network slice SLA data, some information may be exposed if application functions are shared |
| VNF application data and sensitive parameters | The application related data and sensitive parameters associated with a VNF |
|  |  |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0028 | Audit Policy Violations - Automated user and resource policy compliance checks and instrumentation to alert on violation attempts |
| DS0015 | Audit logs - Auditing logs for security, authentication and authorization activity, host access, hosts, virtualization orchestrator and managers can reveal behavioral anomalies |
| DS0013 | Monitor systems performance |
| DS0029 | Monitor network flows |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| Fraunhofer AISEC, “Threat Analysis of Container-as-a-Service for Network Function, accessed April 28, 2021 | https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien\_TechReports/englisch/caas\_threat\_analysis\_wp.pdf |

Notes: