T1599.502 Network Slice Infrastructure 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: Adversaries may use a less secure slice to gain access to information in a more secure slice that uses the VNF (Common VNF) built on common infrastructure to misuse resources allocated to target VNFs or slice.

A compromised (intentionally or simply misconfigured) VNF instantiated in one slice subnet may access resources of another slice subnet. A common Network function Virtualization Orchestrator (NFVO) or Virtualized Infrastructure Manager (VIM) without proper safeguards may allow an adversary to starve a target slice or VNFs of the resources it needs to meet the SLA and to create opportunities information exposure.

Labelling:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Use of common virtual orchestrators and infrastructure managers | If a service provider uses network slicing and creates two slice subnets by creating network service instances on the same NFV environment (i.e. the same NFVO and functional blocks) and thus being built with resources of the same NFVI-PoP(s), this may lead to unauthorized access to resources/data of another slice. |

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 | 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 |
| VNF Lawful Interception (LI) data | LI application server manages user activity monitoring requests and monitoring set up of the user voice calls, SMS and data |
|  |  |

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 |
| ETSI NFV SEC026 Isolation and trust domain specification, section 4.2.3 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC026\_Isolation\_and\_trust\_domain |