T1599.501 Malicious co-tenancy exploit of NFVI (Network Slice)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| July 27 | MV |  |  | Red text new. Moved things around to comply with formatting |
|  |  |  |  |  |

Description: Adversaries may gain unauthorized access to information via a Virtual Network Function (VNF) shared for service designed for two different slices

5G functions deployment and slice creation is supported by NFVI resources. Network Function Virtualization Infrastructure (NFVI) can be exploited by compromise or abuse of trust on a VNF Orchestrator (VNFO) or VNF Manager (VNFM). An adversary may be able to create a network slice (NS) using the VNF (Common VNF) of a target Slice or create slice resources that share the NFVI resources of the target slice. Malicious co-tenancy activities can lead to unauthorized access to data, misuse of resources, or management actions.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Defense-Evasion

Metadata:

* Platform(s): OA&M, Virtualization, Slice
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:
* Architecture Segment: Arch-Slice, Impl-CSP

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Create Malicious Co-Tenancy | A legitimate tenant 1 uses the Os-ma-nfvo interface to read the NS information of another tenant 2 sharing the NFVO. The tenant 1 may get sensitive information on the NS topology for a NS of a competitor (tenant 2). |
| Consume on-boarding resources | A malicious tenant on-boards unused NS/VNF just to consume on-boarding resources (e.g. fill the NS and VNF registries or software image repository) to limit the space available for other tenant. |
| Manipulate network slices of another tenant | A malicious tenant uses the Os-ma-nfvo interface to manage the NSs of another tenant. For example, this malicious tenant may scale down the NS of a competitor to get more resources for his own NS or scale up to increase resource cost of another tenant. |

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, VNF sensitive parameters, |  |
| VNF Lawful Interception 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 4.2.2 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC026\_Isolation\_and\_trust\_domain |

#doNotParse

Sub attacks:

* A legitimate tenant 1 uses the Os-ma-nfvo interface to read the NS information of another tenant 2 sharing the NFVO. The tenant 1 may get sensitive information on the NS topology for a NS of a competitor (tenant 2).
* A malicious tenant on-boards unused NS/VNF just to consume on-boarding resources (e.g. fill the NS and VNF registries or software image repository) to limit the space available for other tenant
* A malicious tenant uses the Os-ma-nfvo interface to manage the NSs of another tenant. For example, this malicious tenant may scale down the NS of a competitor to get more resources for his own NS or scale up to increase resource cost of another tenant

<Following needs to be moved to Network Slice attack>

Two users use their own NFVO and VNFM but allocates resources on the same NFVI-PoP(s) (NFV Infrastructure Point of Presence) to build their NSs (Network Slices). Sub attacks:

-This malicious NFVO or VNFM uses for the instantiation of the VNF the resourceGroupId of the legitimate tenant. This VNF sharing the domain of other VNFs of the legitimate tenant may access to the resources of the legitimate VNFs.

- A malicious NFVO or VNFM request reservation of resources (compute, storage, network) using Or-Vi or Vnfm-Vi interface respectively, to jeopardize the NFVI resources available

- A malicious NFVO uses the Or-Vi software image interface on behalf of a legitimate tenant authorized to access the VIM, to add, delete, update or to query information of Software images from the VIM

- A malicious VNFM uses the Vnfm-Vi software image interface on behalf of a legitimate tenant authorized to access the VIM, to query information of Software images from the VIM

- VNF instantiated in the NFVI accesses to the resources reserved for another tenant and not sharable

- A malicious tenant accesses in the WIM to data transiting between another tenant’s two VNF instances instantiated in two different NFVI-PoPs