T1498.502 Shared slice common control network function resource exhaustion

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: Adversaries may exhaust common resources of a slice to cause denial of service (service degradation) to all other slices that use the same common resources.

5G network slices may be built using same NFVI resources or may be sharing a common Core or RAN function. A network slice may have dedicated AMF, SMF and UPF but NEF, NRF, UDM is usually shared for a deployment. Adversary’s slice A may target a slice B by exhausting resources common to slice A and B such as NEF.

It is possible for adversary’s slice to oversubscribe a resource (NF or NFVI Resource) to an extent where other slices cannot get their messages and process executed in due time. This result in UEs or some network functions experiencing denial of service within target slices.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Impact

Metadata

* Architecture Segment: Slice
* Platform(s): Slice, CSP
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **ID** | Uses |
| Resource Policy enforcement | Create and enforce resource policy; policy can include SLA, quotas, QOS etc. |
| Horizontal Elastic Scale |  |
| M1030 | 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 |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| NFVI | NFVI network and compute resources |
| VNFs | 5G Core, RAN and NON-SBI functions, virtual resources supporting VNF |
|  |  |

Detection

|  |  |
| --- | --- |
| **ID** | **De**tects |
| Audit Policy Violations | Automated user and resource policy compliance checks and instrumentation to alert on violation attempts |
| 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 and alert on quota exceptions on hosts, applications and networks |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC026 Isolation and trust domain specification, section 4.2.3, Accessed 6/27/2022 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC026\_Isolation\_and\_trust\_domain |
| GSMA Official Document NG.126 - Cloud Infrastructure Reference Model\_NG.126-v1.0-2, Accessed 6/27/2022 | https://www.gsma.com/newsroom/wp-content/uploads//NG.126-v1.0-2.pdf |
| UKS: R. Pell et.al, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, Oct. 2021 | https://arxiv.org/abs/2108.11206 |
| NGMN  5G SECURITY RECOMMENDATIONS PACKAGE #2 : NETWORK SLICING, Accessed 6/27/2022 | https://www.ngmn.org/publications/5g-security-recommendations-package-2-network-slicing.html |