T1599.504 Manipulate Virtual Network Function (VNF) Configuration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| July 27, 2022 | MV | Corrected in red |  | Other formatting changes |
|  |  |  |  |  |

Description: Adversaries may bridge network boundaries by modifying a Virtual Network Function’s Configuration.

Any VNF that serves as a Middlebox can be targeted by adversary for configuration exploits (NAT, or GWs, SEPS, IPXs). Configuration stored on the device determines the device behavior for middle boxes such as NAT or application GWs. Start up and run time configuration data can be manipulated for nefarious purposes. SDN VNF unauthorized configuration changes can lead modified 5G traffic flows and may bridge otherwise isolated slices.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: defense-evasion

Metadata:

* Architecture Segment: Virtualization
* Platform(s): SDN vSwitch, Network Element
* Access type required: User or Administrative access to repository
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Active configuration changes | Active configuration changes can be made when direct access to VNF or its element managers is available |
| Stored or Coded configuration | Configuration as a code repository or back up configuration store can be manipulated to cause an NF to take compromised configuration upon reboot or re-instantiation |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1033 | VNF Access Rights -Restricted Permissions to add images to VNFs (Network Element) for person and non-person accounts |
| M1047 | Logs from VNFs must be corelated with other OA&M and Security monitoring tools to ensure unauthorize activity is reported. SEIM like system should be deployed to correlate events. |
| M1053 | Configuration back ups -All VNF Configurations should be backed up and periodically audited to see differences between running configuration and back up configurations as well as comparison between configuration catalogue and running instance |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Credential and Access | Privileged Access to VNF or VNF managers via direct login or thru Control Plane APIs |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| VNF orchestrators, VNF managers, operations, and security tools | Adversary may target a particular network controller, network element, CI/CD, security, and operations tools to manipulate VNF behavior |
| VNF Configuration file | Adversary may target configuration in the VNF, stored in backups, or part of the code |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0028 | Access Logs - Analyze logs to detect unauthorized activity to VNF and other tools used in lifecycle management and security of the VNF |
| DS0015 | Audit configuration - Periodically audit VNF configuration to detect unauthorized changes |
| DS0029 | Audit network flow - Audit network flows to VNF and other tools used in lifecycle management and security of the VNF |
| DS0007 | Image life cycle and runtime events |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unexpected and unusual VNF behavior | VNF compromise can lead to DOS or change in the traffic pattern and paths. |

References:

|  |  |
| --- | --- |
| Name | URL |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |