FGT5013 Malicious VNF Instantiation

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

Description: An adversary may use a fake controller or compromised controller to deploy fake VNFs to collect information from the network.

Instantiation of malicious Virtual Network Functions (VNF) can also be achieved by compromised VIM by inclusion of concealed software within legitimate (Virtual Infrastructure Manager) VIM, or allocating virtual resources for fake instances, or using malicious or compromised identity provider (reuses the same identity for several VNFs with same key pair without knowledge of MANO). Adversary may use malicious attestation server attacks, etc. VNF instantiation may mallow adversary to register VNF with 5G core to launch further attacks.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Discovery, collection
* Platform(s): ICAM, CI/CD, OA&M Tools
* Access type required: User/NPE/Administrative access, compromised Keys/tokens
* Data Sources:
* Theoretical/Proof of concept/Observed:
* Architecture Segment: Impl-OA&M, Impl-Virtualization

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| S0683 | Peirates can deploy a pod that mounts its node’s root file system, then execute a command to create a reverse shell on the node |
| S0600 | Doki was run through a deployed container |
| G0139 | TeamTNT has deployed different types of containers into victim environments to facilitate execution. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1047 | Scan images before deployment, and block those that are not in compliance with security policies. In Kubernetes environments, the admission controller can be used to validate images after a container deployment request is authenticated but before the container is deployed. |
| M1035 | Limit communications with the container service to local Unix sockets or remote access via SSH. Require secure port access to communicate with the APIs over TLS by disabling unauthenticated access to the Docker API, Kubernetes API Server, and container orchestration web applications. |
| M1030 | Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. |
| M1018 | Enforce the principle of least privilege by limiting container dashboard access to only the necessary users. |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Container and Container engines | Container and container engine may expose privileged information to adversary directly from process or thru container engine. |
| Container Management Controller system | In Container management architecture (Kubernetes for example) adversary may use Kublet commands or API proxy to gain access to information and control of the container. |
| NFO | NF orchestrators |
|  |  |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0015 | Audit application logs (NFVO, VIM). Configuration management databases (CMDB) and other asset management systems may help with the detection of computer systems or network devices that should not exist on a network. |
| DS0032 | Monitor container creation, container start events |
| DS0014 | Monitor POD creation and modification events. |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC025, Secure End-to-End VNF and NS management specification  Release 4, section 4.4.3, accessed 6/28/2022 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC025\_Secure\_E2E\_VNF\_&\_NS\_management/NFV-SEC025v0012.zip |