FGT5014 Shared Resource Discovery

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

Description: An adversary running a malicious VNF may identify network resources co-resident on the same physical host.

An adversary may identify a VNF in shared resource by observing protocols or standard ports in use on the node. A hardware and network resource separation is required to provide isolation and protection from an adversary mapping capabilities in the network for certain VNF/VNFc.

Labelling:

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

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. Segment execution environment with node and network. |
| 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** |
| VNF identity | Adversary may identify high value 5G network functions targets for its exploits |
| Network identity | Adversary may identify RAN, CORE or slice VNFs for further expoits. |

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. |
| DS0017 | Monitor command history on VNFs and hosts |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| Network Functions Virtualisation (NFV) Release 4;  Security;Isolation and trust domain specification  Release 4, section 4.2.1, Access 4/12/2022 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC026\_Isolation\_and\_trust\_domain |