T1609.501 Accessing Terminated VNF

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

Description: An adversary may use an NFVI controller to gain access to data from a suspended or stopped VNF to extract sensitive information.

A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment. An unauthorized access to terminated/suspended VNF in NFVI can expose data not erased from a state change process. This may include virtual resources released from a terminated VNF or from a VNF that has released resources after a move or a scaling process. This may also enable inclusion of concealed software in NFVI to prevent the deletion/erasure of data and states of the VNF that has been terminated. Data may include application data, cryptographic keys (service accounts).

Labelling:

* Sub-techniques: none
* Applicable Tactics: Discovery, Credential-Access
* Platform(s): 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 use kubectl or the Kubernetes API to run commands. |
| S0623 | Siloscape can send kubectl commands to victim clusters through an IRC channel and can run kubectl locally to spread once within a victim cluster |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1038 | Use read-only containers, read-only file systems, and minimal images when possible to prevent the execution of commands. |
| 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 and Kubernetes API Server |
| M1026 | In Kubernetes environments, consider defining a Pod Security Policy that prevents pods from running privileged containers |
| M1018 | Enforce authentication and role-based access control on the container service to restrict users to the least privileges required. |

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. |

Detection

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

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC025, Secure End-to-End VNF and NS management specification  Release 4, section 4.4.6, accessed 6/28/2022 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC025\_Secure\_E2E\_VNF\_&\_NS\_management/NFV-SEC025v0012.zip |