T1078.004 Container Management- Unauthorized access

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

Description: An adversary may use privileged accounts of valid, role-based accounts for management services to gain access to network elements.

Internal or external adversary may gain access to management account credentials (e.g. due to weak account management practices) allowing access to VNF containers for persistence, and defense evasion.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Initial-access, Privilege-Escalation, Defense-Evasion, Persistence
* Architecture Segment: Virtualization, OA&M
* Platform(s): Infrastructure, CI/CD & OA&M Tools
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: observed

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| S0683 | Peirates is a post-exploitation Kubernetes exploitation framework with a focus on gathering service account tokens for lateral movement and privilege escalation. The tool is written in GoLang and publicly available on GitHub |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1032 | Use multi-factor authentication for cloud and virtualization OSS accounts used for VNF deployments, especially privileged accounts. |
| M1027 | Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Rotate access keys regularly. |
| M1026 | Review privileged cloud account permission levels routinely to look for those that could allow an adversary to gain wide access. |
| M1018 | Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts. |
| M1017 | Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications. |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Containerized network functions | RAN and Core CNFs |
| Cloud/virtualized container Management controllers | Cloud, Kubernetes, or Openstack administrative controllers |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0028 | Monitor for suspicious account behavior across cloud services that share account. Logon session logs and meta data helps determine if the session was an authorized activity. |
| DS0002 | Monitor user account authentication activity. Monitor the activity of cloud accounts to detect abnormal or malicious behavior, such as accessing information outside of the normal function of the account or account usage at atypical hours. Repeated attempts may be indictive of password guessing or brute force password cracking. Password policies supporting lockout requiring administrative reset may help. |
|  |  |

Post-Conditions

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

References

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC023, Container Security Spec, section 5.4.4  , Accessed 6/27/2022 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC023\_Container\_Security\_Spec/NFV-SEC023v005.zip |
| Peirates | https://github.com/inguardians/peirates |
| Kubernetes Used in Brute-Force Attacks Tied to Russia’s APT28 | https://vulners.com/threatpost/THREATPOST:B25070E6CF075EEA6B20C4D8D25ADBE8 |
|  |  |