T1611 VM and Container Breakout

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

Description: Adversary may be able to break out of VM/Container to host to compromise co-resident tenant VM/Container for discovery and exfiltration and host-based privilege escalation.

VM guest OS may escapes from its VM encapsulation to interact directly with the hypervisor. This gives the adversary access to all VMs and, if guest privileges are high enough, the host machine as well. Although few if any instances are known, experts consider VM escape to be the most serious threat to VM security.

Similarly, a container may also create privileged access to Host file system or execution environment.

5G deployments may include PNFs as well as VNFs. VNFs may be deployed over Type1 or Type2 VMs or as Containers over guest OS, or over a VM. Examples of 5G functions deployed as CNF due to scaling requirements may include 5G Core capabilities of AMF, SMF, UPF and RAN Capabilities of CU, DU, RIC, x-Apps, r-Apps. A container or VM escape can expose control and user plane traffic as well as credentials to allow adversary to further carry out attacks on the network.

Labelling :

* New 5G Technique #: NO
* Modification of Existing ATT&CK Technique # : T1611
* New Sub-Technique(s) of existing technique? No
* Applicable Tactics: Privilege Escalation, Lateral Movement

Metadata:

* Architecture Segment: Virtualization-OA&M, VNF
* Platforms: Windows, Linux, MacOS
* Permissions Required: User, Administrator
* Data Sources: <needed to drive the detections listed below>
* Theoretical/Observed: Yes

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| S0600 | Container was configured to bind to the host root directory |
| S0601 | Hildegard used the BOtB tool that can break out of Container |
| S0683 | Peirates can gain a reverse shell on a host node by mounting the Kubernetes hostPath. |
| S0623 | Siliscape maps the hosts’s C drive to the contianer by creating a global symbolic link of NtSetInformationSymbolicLink |
| G0139 | TeamTNT has deployed privileged containers that mount the filesystem of victim machine |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1048 | Consider utilizing seccomp, seccomp-bpf, or a similar solution that restricts certain system calls such as mount. In Kubernetes environments, consider defining a Pod Security Policy that limits container access to host process namespaces, the host network, and the host file system |
| M1038 | Use read-only containers, read-only file systems, and minimal images when possible, to prevent the running of commands. |
| M1026 | Rootless containers: Ensure containers are not running as root by default. In Kubernetes environments, consider defining a Pod Security Policy that prevents pods from running privileged containers. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| VNF, CNF | Any capabilities deployed as VNF or CNF |
| VM, Contianer host | Host OS, VM host server becomes a bridging device between tenant VMs and Containers if compromised |
| Credentials | In addition to application data exposure, credential exposure is usually a key target for adversary to open the doors for many other exploits. |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0009 | Monitor process creation and OS API execution activity. |
| DS0032 | Monitor for the deployment of suspicious or unknown container images and pods in your environment, particularly containers running as root. |
| DS0034 | Monitor cluster-level (Kubernetes) data and events associated with changing containers' volume configurations. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC023, Container security spec (WIP) v004. | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC023\_Container\_Security\_Spec |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | https://arxiv.org/abs/2108.11206 |
| Github, “Awesome VM exploit” | https://github.com/WinMin/awesome-vm-exploit |
| Project Zero | https://googleprojectzero.blogspot.com/2021/06/an-epyc-escape-case-study-of-kvm.html |