FGT5004.002 vSwitch

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

Description: An adversary may compromise a vSwitch in an SDN network to manipulate the network traffic or cause denial of service

An SDN vSwitch is like a layer 2 switch that connects devices to the network and performs packet forwarding between the switch ports. This threat involves compromising an SDN vSwitch (an SDN device responsible for packet/data switching between different ingress and egress ports) to forge network data and launch other attacks (e.g., DOS). Adversary may target vSwitch configuration or directly manipulate network flow tables in memory to drive their decisions on how to redefine large parts of the network.

Labelling:

* Sub-techniques: No Sub-Techniques
* Applicable Tactics: collection, discovery

Metadata:

* Architecture Segment: Impl-Virtualization
* Platform(s): SDN vSwitch, Network Element
* Access type required: User or Administrative access to repository
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1022 | Restricted Permissions to add application images to SDN vSwitch for person and non-person accounts.  Restricted permissions for person and non-person accounts to prevent flow rule insertion or modification directly on the vSwitch |
| FGM5091 | Mutual authentication between SDN controller and vSwitch can prevent unauthorized access |
| FGM1557 | Strong integrity protection method should be employed on APIs carrying control plane traffic between Controller and network element as well as controller and vSwitch to avoid adversary in the middle threats |
| M1041 | Strong encryption should be used on APIs carrying control plane traffic between Controller and network element as well as controller and vSwitch to avoid adversary in the middle threats |
| FGM5090 | Logs from SDN Controller and network elements must be corelated to ensure unauthorize activity is reported. Similarly flow rules change log should be reviewed and reconciled with authorized changes. |
| M1053 | SDN vSwitch configurations should be backed up and periodically audited to see differences between running configuration and back up configurations |
| M1054 | Keep baseline configuration up to date to avoid loopholes due to stale configuration or configuration drift. |
| M1030 | Physical and logical segmentation can prevent lateral movements. Segmentation techniques in the hosts and network will reduce the chances of lateral movement to the control. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Credential and Access to SDN vSwitch | Privileged Access to SDN vSwitch via direct login or through SDN control plane APIs |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SDN vSwitch, operations, and security tools | Adversary may target a particular network controller, network element, CI/CD, security, and operations tools to manipulate SDN network flows in a vSwitch |
| SDN vSwitch Configuration file | Adversary may target configuration to manipulate vSwitch and network behavior |
| SDN vSwitch flow table | Network flows are stored in Network Flow tables, usually refer to as route or switch tables that vSwitch uses to decide which packet forwarding port to use for incoming packets |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGDS5014 | Analyze logs to detect unauthorized activity |
| DS0015 | Periodically audit SDN and Network element configuration and compare with baseline configuration to detect unauthorized changes |
| DS0029 | Periodically audit network flow tables to detect unauthorized changes to flow data |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Network flow compromise | Network flow compromise can lead to DOS, or change the traffic pattern and paths. Adversary may change the path for network sniffing or for MiTM activity. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| ENISA, “Threat Landscape and Good Practice Guide for Software Defined Networks/5G”, Jan. 2016 | https://www.enisa.europa.eu/publications/sdn-threat-landscape |
| Scott-Hayward, S., O'Callaghan, G., & Sezer, S. “SDN Security: A Survey”. 2013 IEEE SDN for Future. Networks and Services (SDN4FNS) (pp. 1-7) | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6702553&tag=1 |
| 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 |