FGT5004.001 Controller

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

Description: An adversary may use the compromised SDN controller or Control plane API to modify network flow rules, or traffic management policies.

An SDN controller is a centralized control application for policy, device configuration, and traffic flow management. SDN controller compromise can allow an adversary to change the traffic path for offensive or defensive evasion purposes as well as cause denial of service to certain networks or end points. SDN Controller application is typically installed on a physical over virtual server and communicate northbound to other OAM applications as well as southbound to network switches. SDN controller acts as an Operating System for the Network in SDN architecture and is widely deployed in data centers and wide area network connections (SD-WAN).

Labelling:

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

Metadata:

* Architecture Segment: Impl-Virtualization
* Platform(s): SDN Controller
* 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 Controller for person and non-person accounts.  Restricted permissions for person and non-person accounts to prevent flow rule insertion or modification |
| FGM5091 | Mutual authentication between SDN controller and network elements, SDN controller and SDN application 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 SDN application 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 SDN application 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 controller 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 Controller | Privileged Access to SDN controller via direct login or through SDN control plane APIs |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SDN Controller and Network Elements, operations, and security tools | Adversary may target a particular network controller, network element, CI/CD, security, and operations tools to manipulate SDN network flows. |
| SDN controller Configuration file | Adversary may target configuration to manipulate controller and network element behavior |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGDS5014 | Analyze logs to detect unauthorized activity |
| DS0015 | Periodically audit SDN and Network element 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 |