FGT5004 Network Flow Manipulation

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

Description: An adversary may discover Software Defined Network (SDN) flow information, which could then be used for lateral movement and unauthorized changes in the network.

To achieve this, an adversary must compromise an SDN element (e.g., controller, router, switch) to forge network data and launch other attacks, such as denial of service. While data forging could relate to data held by any component of an SDN (e.g., network switches, controllers and/or SDN applications), a threat specific to SDN consists of forging requests from accessible low level SDN controllers to upper-level ones. This could then drive the upper level controllers’ decisions on how to redefine large parts of the network. In the literature, this scenario has been identified as a threat related to components in the data plane and the controller plane of any SDN network (IP-WAN, IP-LAN, RAN, Transport).

Labelling:

* Sub-techniques: FGT5004.001, FGT5004.002
* Applicable Tactics: collection, discovery

Metadata:

* Architecture Segment: Virtualization
* Platform(s): SDN
* 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 images to SDN Controller and Network Elements for person and non-person accounts.  Restrict permissions for person and non-person accounts to prevent flow rule insertion or modification |
| FGM5091 | Mutual authentication between the SDN controller and network elements. The SDN controller and SDN application can be used to 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 | All SDN Configurations should be backed up and periodically audited to see differences between running configuration and back up configurations |
| M1054 | Keep baseline configurations up to date to avoid loopholes due to stale configuration or configuration drift. |
| M1030 | Physical and logical segmentation can prevent lateral movements. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Credential and Access to SDN Controller and network elements | Privileged Access to SDN controller and Network elements |

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 Configurations file, Network flow tables | Adversary may target configuration or network flow data |

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=6702c553&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 |