FGT5005 Memory Scraping

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

Description: An adversary may be able to read memory registers to discover privileged information such as local password comparison, encryption key etc.

An adversary can achieve this by scanning the physical memory used by a given software program. This will give the adversary access to any information that the program has access to, which could be sensitive. While memory scraping can affect components of any layer of the network, this type of threat has been primarily a focus of SDN application servers where the adversary can have greater advantage, if successful, in discovering sensitive information (credentials such as token and keys).

Adversaries may use memory scraping to target different components of the core network, a core dump of an SDN controller (e.g. as the result of malicious software) can be used to exploit private data. Once successfully performed, memory scraping can be used to extract sensitive SDN data (e.g. flow rules at the northbound API).[2]

Labelling:

* Sub-techniques: none
* Applicable Tactics: collection

Metadata:

* Architecture Segment: Impl-Virtualization
* Platform(s): SDN, Hosts
* Access type required: Administrative access, Access to install scraper malware
* Data Sources:
* Theoretical/Proof of concept/Observed: Observed

Procedure Examples: Target breach,

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | Many memory scrapers exist on the darkweb with varying features, including camouflage, self-destruction and C2 connections. Malware delivery is similar to other malware, but attacker scans network for right target for SDN controller or target host. A few Malware examples include Dexter, Soraya, ChewBacca and BlackPOS. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1033 | Restrict permissions to add software to SDN controller and network elements for person and non-person accounts |
| FGM5090 | Logs from SDN controller and network elements must be correlated to ensure unauthorize activity (file transfer, patch installs, process init) is reported. |
| M1047 | SDN controllers and network elements scanned for file changes and processes. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Credential and access to SDN controller and network elements | Privileged access to SDN controller and network elements to transfer and install malware to the target host. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SDN controller and network elements (or any target host) | Adversary may target a particular network controller, network element, CI/CD, security, and operations tools to collect data |
| SDN configurations file, Network flow tables | Adversary may target configuration or network flow data |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0015 | Analyze logs to detect unauthorized activity |
| DS0029 | All inbound and outbound connections should be audited for unauthorized activity |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, section 6.2, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| ENISA, “Threat Landscape and Good Practice Guide for Software Defined Networks/5G”, Jan. 2016 | https://www.enisa.europa.eu/publications/sdn-threat-landscape |
| ETSI GS NFV-SEC 009 V1.1.1, “NFV Security:  Report on use cases and technical approaches for multi-layer host administration”, December 2015 | https://www.etsi.org/deliver/etsi\_gs/nfv-sec/001\_099/009/01.01.01\_60/gs\_nfv-sec009v010101p.pdf |
| N. Huq, “PoS RAM Scraper Malware: Past, Present, and Future,” Trend Micro, accessed May 25, 2023 | https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf |
| J. Hizver, “Taxonomic Modeling of Security Threats in Software Defined Networking”, Blackhat Conference, Aug. 2015 | https://www.blackhat.com/docs/us-15/materials/us-15-Hizver-Taxonomic-Modeling-Of-Security-Threats-In-Software-Defined-Networking-wp.pdf |
| 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 |