FGT5007 Registration of malicious network functions

Description: An adversary, such as an insider to the MNO or vendor, may install a malicious NF into the core network, in order to launch other attacks or get access to information.

An adversary could introduce an unauthorized network function (NF) or function embedding trojan malware in the service base architecture (SBA) by registering it in the NRF, in order to exploit other APIs. A clone of a legitimate NF can also be used to register itself in the NRF. The new NF can be deployed as a PNF, cloud VNF or containerized NF. This adversary could be an insider (to the MNO) or a vendor or service provider. By having an unauthorized network function installed or activated, an adversary may gain access to resources in the network to perform other type of attacks such as Denial of Service, the distribution of malicious software, or obtaining sensitive information.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Execution

Metadata:

* Architecture Segment: OA&M, Control plane
* Platforms: 5G
* Access type required: admin
* Data Sources:
* Theoretical/Proof of Concepts/Observed: Theoretical.

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Unauthorized use of API | Rogue or cloned NF calls Nnrf\_NF Management API to register one of these functions: AMF, SMF, UDM, AUSF, NEF, PCF, SMSF, NSSF, UPF, etc. Clause 5.2.7 of [3] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM1506 | Cross check newly registered NFs. Out of band mechanism for cross checking new NFs that are registered in NRF are as expected by network administrator. NRF may use additional OAuth2.0 token information. |
| M1018 | User account access |
| M1030 | Network segmentation |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Network services | Network services provided to UEs. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Monitor application logs of core NFs. |
| DS0032 | Monitor for newly constructed containers that may deploy a container into an environment to facilitate execution or evade defenses. |

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** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, November 2019. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks |
| 3rd Generation Partnership Project (3GPP) TS 23.502, “Procedures for the 5G System (5GS); Stage 2 (Release 17)”, Technical Specification, v17.4.0, March 2022. | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

Background info:

