T1499 Public Function Denial of Service

Description: An adversary may exploit weaknesses in Application Programming (API) interfaces on Network Functions (NF) that are exposed to the public, i.e. Internet which exposes those functions to potential adversary denial of service of the NF.

Some 5G functions such as the NEF have API’s that are public facing and are subject to potential exploit by adversaries similarly to public facing websites and services. The adversary could exploit a previously identified weakness in the API to cause the NF to crash resulting in denial of service. The adversary may also potentially use volumetric techniques to degrade or deny service.

Labelling:

* Sub-Techniques: None
* Applicable Tactics: Impact

Metadata:

* Architecture Segment: Control-plane, User-plane
* Platforms: 5G
* Access type required: N/A
* Data Sources: Network Flow Logs, Application Logs
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Vulnerability Exploit | Adversary uses a vulnerability to cause the NF to crash |
| Volumetric attack | Adversary uses one or more volumetric techniques to degrade or deny availability of the NF |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1016 | Vulnerability scanning of public APIs |
| M1050 | Use WAF to minimize potential exploit of vulnerabilities |
| M1037 | Use of network based DDoS mitigation capabilities to filter traffic upstream |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| API vulnerability | Adversary may need to identify vulnerabilities in the API to obtain initial-access, unauthorized information, or perform a denial of service |
| API credentials | Adversary may need to obtain credentials to collect unauthorized information |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| NEF | Network Exposure Function which provides API access to Application Functions (AF) |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Monitor application logs for unusual requests or rate of requests |
| DS0029 | Monitor for unusual volumes or sources of requests to the service |
|  |  |

Post-Conditions

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

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 |
| 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 |
| TOP 7 REST API Security Threats, blog January 2019 | https://blog.restcase.com/top-7-rest-api-security-threats/ |

*#doNotParse*

From ENISA:

