T1190 Exploit Public-Facing Network Function

Description: An adversary may exploit weaknesses in Application Programming (API) interfaces on Network Functions (NF) that are exposed to the public Internet, which exposes those functions to compromise of the NF, or disclosure of information.

Some 5G functions such as the NEF have APIs 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 gain initial access to the operator’s environment. The adversary may also obtain credentials through other techniques that allow the adversary to obtain unauthorized information from the exposed network function. See [FGT5029 - Exploit Semi-public Facing Application] ( /techniques/FGT5029/) for API exposure to interworking networks.

An example of this is represented through access control of application functions (AF) by NEF is done at the API level which is not protected at a granular enough level, i.e., it is not done at IE level. An adversary may use a AF to make requests for a service, e.g. location of a UE, beyond their authorization level since IE’s are not explicitly required to be checked.

Labelling:

* Sub-Techniques: None
* Applicable Tactics: initial-access, collection

Metadata:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |
| Sensitive data exposure | Adversary uses an insecure API to take over the edge NF, then can use legitimate signaling to obtain sensitive UE or network data. |
| Exploit vulnerable API | Adversary may bypass standard AF API access control mechanism by using crafted IEs to access sensitive data such as location of a UE through a NEF |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1016 | Vulnerability scanning of public APIs |
| M1050 | Use WAF to minimize potential exploit of vulnerabilities |

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 |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
|  |  |

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/ |
| OpenUPF, ”Deployment Scenarios of Private 5G Networks,” October 13, 2022 | https://www.openupf.net/en-us/docs/7private5gdeploy.html |

*#doNotParse*

From ENISA:

