FGT5011 Unauthorized access to Network Exposure Function (NEF) via token fraud

Description: An adversary controlling an (external) Application Function (AF) may present a fraudulent OAuth access token to access Network Exposure Function (NEF) services.

A mobile network operator has access to a variety of user and network data by virtue of the services it provides to subscribers. As a business extension, some of these capabilities, events and data can be offered to other partner business entities. The Network Exposure Function securely exposes such cellular network services to authorized third-party applications. The standard mandates TLS between NEF and AF and authorization via OAuth 2.0.

Examples of the data that can be shared are: device analytics, user traffic routing, device location and mobility events: for example, notifications are sent whenever a user (which is e.g. part of a group subscribed to a third party service) enters a certain geographical perimeter (e.g. a mall or campus), since the operator keeps track of the base stations to which devices are connected.

A malicious AF with a fraudulent (stolen, altered, or constructed) access token may invoke the NEF services arbitrarily.

Labelling:

* Sub-technique(s):
* Applicable Tactics: lateral-movement, initial-access

Metadata:

* Architecture segment: Arch-ICAM, Arch-Control plane
* Platforms: 5G Network
* Access type required: admin
* Data Sources:
* Theoretical/Proof of Concept/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 |
| OAuth 2.0 attacks | An adversary may conduct OAuth2.0 attacks that are applicable to machine-to-machine communication (not email phishing type attacks). Fraudulent token is mentioned in section I.2.2.2 of [1]. Other threats are listed in [2]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| M1040 | Prevent suspicious API calls |
| FGM5003 | Ensure NEF checks AF credentials across layers (TLS, OAuth2.0), and has a list (provided out of band) with all the allowed AF by unique identifier (or type of AF), and to which service they are allowed access (this access may be general, not per UE). |
| FGM5019 | NEF should authorize API calls from external AFs for all service accesses, via OAuth token verification. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| MNO service access | Access to some MNO services to gain knowledge about tokens to access the NEF |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |
| Operator Services | Network services exposed by NEF |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Logs of connection attempts to NEF |

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) |
| Network services exposed by NEF | Adversary has access to network services exposed by NEF |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 3GPP TR 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes. | https://www.3gpp.org/DynaReport/33926.htm |
| Internet Engineering Task Force, IETF RFC 6819 “OAuth 2.0 Threat Model and Security Considerations”, Jan. 2013. | https://datatracker.ietf.org/doc/html/rfc6819 |

#doNotParse

Background information on NEF from NIST SPECIAL PUBLICATION 1800-33B draft

NEF acts as a secure gateway to trusted (internal) and untrusted third-party (external) application functions (AFs) for exposing various services such as analytics, user traffic routing, UE location, reachability, and mobility-related information. It authenticates and authorizes services requested by the AFs. 5G standards mandate integrity, replay, and confidentiality protection for communication between the NEF and AFs. 5G standards also mandate NEF to AF connection to support TLS and use of certificate-based mutual authentication between third-party AFs and NEF. NEF masks sensitive 5G network information such as DNN, S-NSSAI, and sensitive subscriber information such as SUPI from the third-party AFs.