FGT5003 Network Function Service discovery

Description: An adversary may query the Network Repository Function (NRF) to discover restricted Network Function (NF) services to further target that NF.

All active NFs in an operator network are to be securely registered with the NRF. Part of this registration information includes the type of NF, the particular services it provides, IP addresses, etc.

Consumer NFs query the NRF for Producers NFs they need to interact with, but the NRF is expected to check that the Consumer NF is authorized to discover such Producer NF. This type of signaling to the NRF can be abused to identify and target the NF of interest. The NRF is expected to check discovery request against senders profile, which is prone to misconfiguration and thus might not protect the restricted NF services.

In network slicing, the same principles of NRF apply, and the service discovery is restricted per slice; however, NFs in one slice may have a legitimate need to communicate with NFs in another slice. If NF discovery authorization for a specific slice is not supported by the NRF, the NF instance in one slice can discover NF instances belonging to other slices. For example, an NF in one slice should not be inquiring about NFs in other slices, unless it needs to communicate with them.

Labelling:

* Sub-techniques: None
* Applicable Tactics: Discovery

Required

Metadata:

* Architecture Segment: Control plane, Slice
* Platforms: 5G Network
* Access Type Required: token
* 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 |
| Access token abuse | A malicious NF can abuse access token issued by the NRF for one slice to access another shared NF in a different slice. Clause H.2.2.1 of [2] |
| Access token hijack | Access tokens can be hijacked by a compromised intermediate reverse proxy server such as SCP (if deployed by operator). This attack can be followed by re-direct or replay or access tokens. Section 3.9 of [3] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| FGM5003 | Ensure cross-layer checks at the NRF, between the certificate presented to it at the TLS connection setup stage and the identity and authorization requested presented to it at the OAuth Token request stage.  Ensure the consumer is authorized to ask about this service.  Authorization follows need-to-know rules, such as:  1. a NF can not query for NFs in other network slices  2. a NF can only query for NFs that it needs to communicate with. |
| FGM5501 | Inspect proxy servers such as SCP (if deployed) for any suspicious use of access tokens such as unauthorized re-direct or replay of tokens |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access to NRF | NRF is by design open to connections from other network functions. Control of another NF in the operator domain may be required. |
| Access to SCP | SCP is compromised to hijack tokens. |

Critical Assets

|  |  |
| --- | --- |
| **ID** | **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 network components and services | It is possible for example to find out whether an operator provides services to a certain customer. Or whether a user is also part of a private slice e.g. DOD. There is slice isolation assurance loss with this threat. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Logging of all access requests/inquiries |

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) |
| Unauthorized probing of network services | Information of what other services are provided by a given MNO |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| 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 |
| 3GPP Technical Report 33.926, “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, Release 17. | https://www.3gpp.org/DynaReport/33926.htm |
| Internet Engineering Task Force (IETF) “OAuth 2.0 Security Best Current Practice”, draft-ietf-oauth-security-topics-05, June 2022. | https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics-19 |