FGT5012.005 Shared network function in slice

Description: An adversary may use a legitimate access token for a shared Network Function (NF) to get location info of a user of a different slice.

An adversary controlling a slice or a NF in a slice obtains an access token for a shared 5G core NF (e.g., AMF) and uses it to get location info for an SUPI of a user belonging to a different slice but still served by same NF.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Discovery, Collection

Metadata:

* Architecture segment: Slice, Control-plane.
* Platforms: 5G core
* Access type required: User/Admin of slice
* 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 |
| Malicious NF belonging to compromised Network Slice gets an access token for the target AMF, which serves both target slice and compromised slice. | Malicious NF of a compromised slice gets access token for a shared AMF, but then asks AMF for the location of a UE in the target slice. The AMF checks that the authorization (OAuth) token is ok, which it is, but does not check that the UE ID is served by target slice, while the requester NF is from compromised slice. Section 3.1.5 of [1]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5012 | Cross check requested SUPI is served by (belongs to) the slice ID (NSSAI) of the consumer NF (and presented in the authorization Token). That is, this attack could be mitigated if the shared network function (NF service producer) checks the SUPI in a service request and the requesting NF service consumer are being served by the same slice. (3GPP SA3 is investigating if 3GPP specifications allow for such check) |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access shared NF in a different slice | Two slices share one common NF that is able to get UE location info. Adversary has control of one slice or at least a NF in that slice -- where said NF is allowed to talk to the AMF.  The following core NFs can legitimately ask for or obtain directly the location of a UE (some granularity): AMF, UDM, NEF, NWDAF, GMLC, LMF. The following core NFs can only get limited/coarse location: SMF, UPF, PCF. |

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. |
| UE location | UE/Subscriber geographical location, coarse or fine-grained |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Regularly audit applications and interface messaging logs. Check logs of requests/responses at the shared NF. E.g., each entry should contain SUPI, NF consumer that requested it, slice IDs of both. |

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) |
| UE’s location is tracked by rogue NF | Target slice information is leaked, slice confidentiality is breached due to sharing the NF between slices. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| AdaptiveMobile Security, "A Slice in Time: Slicing Security in 5G Core Networks", 17032021-v1.00, March 2021. | https://info.adaptivemobile.com/network-slicing-security |