FGT5027 Spoof network slice identifier

Description: An adversary controlling a Network Function (NF) or slice can gain access to a different network slice data by interacting with other NFs.

Every network slice has an identifier, part of which is sensitive just like a UE permanent identifier. If this Slice Differentiator (SD) is discovered, then a malicious NF and/or malicious slice can use the guessed SD to gain unauthorized information or resource access to that victim slice. This is done by tricking the NRF to issue a token for a slice that the requestor NF is not authorized to access, then using that token to get information from the shared NF. It is assumed that the shared NF is serving both own slice and the victim slice.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Defense-evasion, Collection

Metadata:

* Architecture segment: Slice
* Platforms: 5G network
* Access Type Required: N/A
* 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 |
| Adversary NF in one slice uses guessed slice identifier of another slice to gain unauthorized access to resources in that slice. | A malicious NF and/or malicious slice can use the guessed identifier Slice Differentiator (SD) to gain unauthorized information or resource access to a different slice. The NF asks the NRF for an OAuth token for an NF in that other slice. The reason is the requested SD (actually, the entire NSSAI) is included in the OAuth token without verification whether requester is allowed access to it. The NRF issues that OAuth token because it is for a producer NF that serves both the requester’s slice and the targeted (victim) slice.  This seems to be a poor approach to access control- one that relies on knowing an identifier, and so access is given if that identifier—presumably kept secret—is found out. See section 3.1.3.1 of [1]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5003 | The attack can be mitigated if the NRF performs additional checks. The NRF authorizes the NF service consumer to obtain tokens only for authorized slice(s). (3GPP SA3 investigating as of early 2022). A cross check with the TLS certificate of requester should be performed as well at the NRF. |
| M1020 | Inspect TLS layer encryption |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Slice identifier was discovered | See [FGT5028](/techniques/FGT5028) |
| Two slices share one common NF | This is common in practice |
| NRF does not check requester slice identifier and the target (consumer) slice identifier. | This is implicit in the standards that do not mandate this check. |

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. |
| Confidentiality of slice-specific resources | UE (served by that slice) related information. Slice specific configuration – e.g. what NFs are part of it and SLAs of the slice. |
| Core NFs | The functionality of *any* core NF that is shared between slices (AMF, SMF, PCF,.. ) |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Check logs of requests/responses at the shared NF. E.g., each entry should contain UE ID (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) |
|  |  |

References

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

#doNotParse

*Background info:* In and before Release 16, Slice Differentiator (SD) part of the slice identifier (“NSSAI”) was not mandatory and random. Hence “brute forcing” or "enumeration" can be used to guess the SD. If the SD is discovered via these methods, then a malicious NF and/or malicious slice can use the guessed SD to gain unauthorized information or resource access. The reason is the requested NSSAI is included in the OAuth token without verification whether requester is allowed access to it. The NRF issues that OAuth token because it is for a producer NF that serves both the requester’s slice and the targeted (victim) slice.

This seems to be a poor approach to access control- one that relies on knowing an identifier, and so access is given if that identifier—presumably kept secret—is found out.