FGT5028 Discover network slice identifier

Description: An adversary may guess the identifier of a different network slice, which allows for follow-on behaviors against that slice that require that identifier.

The NSSAI is a slice identifier. It contains two elements: a slice service type (four 3GPP defined values) and a Slice Differentiator (SD), which should be unique within that type. Consumer NFs may need to access services of Producers NF belonging to a different slice. Any “consumer NF” can ask the Network Repository Function (NRF) for an OAuth token towards this goal, but it must include the Slice identity-- which contains a SD – in the request.

In Release 16 or earlier, the SD was not mandatory and random. Hence “brute forcing” or "enumeration" can be used to guess the SD. Thus if the consumer NF is compromised and wants to discover other slice IDs, it can ask the NRF for OAuth tokens but with guessed slice identities, until a valid one is returned.

Labelling:

* Sub-technique(s): None
* Applicable Tactics: Discovery

Metadata:

* Architecture segment: Slice
* Platforms: 5G
* Access Type Required:
* 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 |
| An adversary in control of a network function asks the NRF for a token for a guessed SD until a legitimate response is received. | Any “consumer NF” can ask the NRF for information with a guessed slice identifier, until a non-error response is returned. The NRF services that are candidates for this operation are ([2]): discovery and Access token (Nnrf\_NFDiscovery and Nnrf\_AccessToken). For the Discovery service, in the GET NF instances, the parameters can be included “plmn-specific-snssai-list”, which contains the S-NSSAIs that are served by the NF supposedly being discovered. Then the 200OK result contains the NFProfile, which includes the S-NSSAIs. Section 3.1.3 of [1]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5499 | NRF protection against brute-force attacks. NRF should not respond to requests after a given number of failed NSSAI lookups (See detections) |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Compromise of core consumer NF | For NF discovery service, clause 5.2.7.1 of [3] lists the following service consumers: AMF, SMF, PCF, NEF, NSSF, SMSF, AUSF, CHF, NRF, NWDAF, I-CSCF, SCSCF, IMS-AS, SCP, UDM, AF, DCCF, MBSF, 5G DDNMF, TSCTSF. |

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. |
| Slice-specific resources | Confidentiality of slice specific resources |
| AMF and UDM | AMF and UDM have NSSAI information. AMF requests and UDM responds. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0015 | Logs at the NRF of failed NSSAI lookups. If a NF asks for NSSAIs that do not exist, then flag that or take action.  AMF can ask the UDM about NSSAIs legitimately. Keep AMF and UDM logs of transactions involving asks about NSSAIs |

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 disclosure of SD/NSSAI | Now the adversary knows the SD of a given slice it is not authorized to contact. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| AdaptiveMobile Security, "A Slice in Time: Slicing Security in 5G Core Networks", 17032021-v1.00. | https://www.adaptivemobile.com/products/5g-security |
| 3rd Generation Partnership Project (3GPP) TS 29.510, “; Network function repository services; Stage 3”, v17.4.0, Dec 2021. | https://www.3gpp.org/DynaReport/29510.htm |
| 3GPP TS 23.502 “Procedures for the 5G System (5GS); Stage 2” | https://www.3gpp.org/DynaReport/23502.htm |

#doNotParse

Background info:

The NSSAI is a slice identifier. It contains two elements: a slice service type (four 3GPP defined values) and a Slice Differentiator (SD), which should be unique within that type.

The NRF contains the profiles of core NFs. Part of each NF profile may be the slice info, e.g. what slices it can support or it belongs to: supportedNSSAI, roamingNSSAI, allowedNSSAI.

Consumer NFs may need to access services of Producers NF belonging to a different slice. Any “consumer NF” can ask the NRF for an OAuth token for this goal, and include the Slice identity, which contains a SD. Thus if the consumer NF is compromised and wants to discover other slice IDs, it can ask the NRF for OAuth tokens but with guessed slice identities, until a valid one is returned.